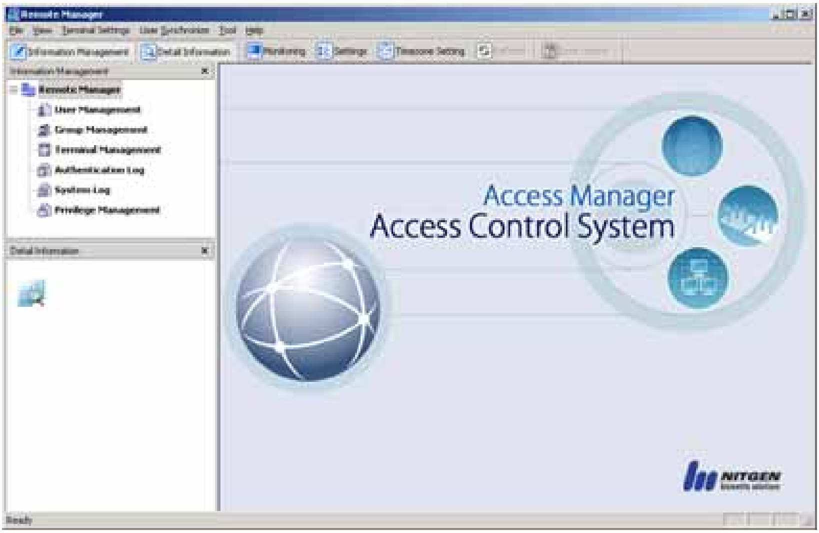
# Access Controller

## NAC-3000 / NAC-2500

## SOFTWARE MANUAL



NITGEN
biometric solutions

- Features and specifications are subject to change without notice. No part of this guide may be copied or reproduced for any purpose without the prior written authorization from NITGEN.
- NITGEN holds the copyright on the brands NITGEN and NITGEN logo.

## To Contact Us

Tel. 82-31-451-9400
Fax. 82-31-451-6723
E-mail: customer@nitgen.com
URL: http://www.nitgen.com

# Table of Contents

# Chapter 1
# Before You Start

## 1.1 About the product

### ■ Overview

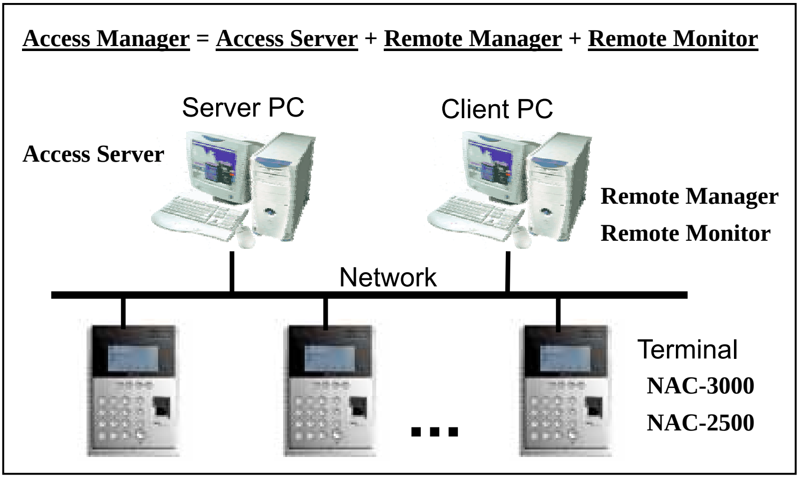
Biometric systems are recently used in various authentication systems. They are increasingly used not only in environments that require high level of security but also in many other places because they are convenient and economical. Among various biometric systems, the fingerprint recognition system takes up most of the market because it is easy to use as well as economical and capable of developing various types of applications. NITGEN, a global leader in the fingerprint recognition industry, provides various fingerprint authentication solutions such as PC security, knowledge management, vaulting service, access control, electronic approval, and financial payment. NITGEN actively responds to customer needs through continuous research, development and quality management.

The NITGEN access control system is an advanced product in which core technologies of NITGEN recognized worldwide such as fingerprint recognition algorithm, optical sensors, embedded design technology, and software application technology are organically combined and optimized. In addition, unlike other existing access control systems that use passwords or ID cards only, it is free from such risks as loss of password and abuse or duplication of card, providing excellent convenience and security. It is designed to maximize operational efficiency, enabling integrated monitoring and systematic management of terminals which have been operated independently on a remote location via the network.

The NITGEN access control system can use various combinations of RF card, password and fingerprint authentication. Designed to meet both universal uses and specific uses, it can be used in various customer environments including enterprises and government agencies due to such convenient built-in features as group ID, short ID, 1:N Authentication, interphone and voice instruction.

This manual describes how to install and use Access Manager that can monitor and manage terminals in connection with the access control terminal (NAC-3000, NAC-2500)

## ■ Product configuration



| Component | Main Features |
|---|---|
| Server PC | 1. Server s/w: Access Sever<br>2. Terminal communication and log data collection<br>3. User information and log database<br>4. Performing authentication |
| Client PC | 1. Client s/w: Remote Manager/Remote Monitor<br>2. User registration and management<br>3. Monitoring terminal status and events |
| Terminal (NAC-3000, NAC-2500) | 1. Performing user authentication<br>2. Door control |

You can use all features with the NITGEN access control terminal (NAC-3000, NAC-2500) only. If you use it with Access Manager in network environment, you can manage a number of terminals more easily and efficiently. You can also use the server and client software in one PC.

## ■ Functionality that is not supported when using NAC-3000 and NAC-2500 in combination.

There are some functionality that is not supported when using the proram with NAC-3000, yet these will be supported in later versions.

The following explains functionality that is not supported when using NAC-3000. Note that all these functions are available with NAC-2500.

| Function | Details |
|---|---|
| Timezone | Supported. But, you don't use the time that a entry is always opened. |
| Anti Pass Back | Anti Pass Back function not supported. |

NAC-3000 terminal: maximum 4,000 users to be stored.

NAC-2500 terminal: maximum 780 users to be stored.

## ■ Main specifications

| Section | Content |
|---|---|
| Access terminal | Connection allowed up to 255 terminals |
| Connection | Simultaneous server access up to 8 Clients |
| Number of users to register | 10,000 users |
| Network | 10 Mbps, TCP/IP |

| | |
|---|---|
| Authentication type | Fingerprint, password and RF card (optional) |
| Algorithm ( Fingerprint ) | FRR: 0.1 % or less, FAR: 0.001 % or less |
| Authentication speed | 1:1 mode: Less than 1 second<br>1:N mode: Avg. 2.5sec ( 1,000FP , Server )<br>Avg. 2sec ( 500FP, Terminal )<br>Avg. 1sec ( 300FP, Terminal )<br>* Pentium IV 1 GHz, 512 MB RAM |

## ■ System environment

- Server system (Access Server)

| Section | Content |
|---|---|
| O/S | MS Windows 98SE/ME/2000/XP/2003<br>( Winows 2000 or later Recommended ) |
| CPU | Pentium III 500 MHz or later<br>(Pentium IV 1 GHz or later Recommended) |
| RAM | 128 MB or more<br>( 256 MB or later Recommended) |
| Hard disk space | 5 GB or more |
| Database | MDB / MS-SQL (available in later versions)<br>( Regard to the manual “MSSQL Setup Guide”. ) |

• Client system (Remote Manager/Remote Monitor)

| Section | Content |
|---|---|
| O/S | MS Windows 98SE/ME/2000/XP/2003 |
| CPU | Pentium II or later |
| RAM | 64 MB or more |
| Hard disk | 1 GB or more |

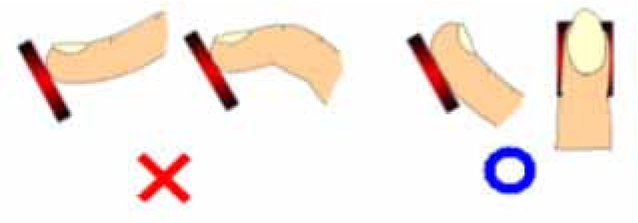
• Fingerprint recognition device (USB Type)

To authenticate manager fingerprint or enroll user fingerprint on a PC, you must install the NITGEN fingerprint recognition mouse (MFDU01), or the fingerprint recognition hamster (HFDU01).

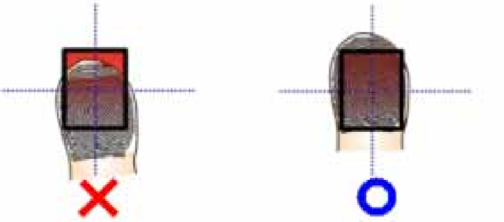
## 1.2 How to input fingerprint

When you enroll and authenticate user fingerprint, do the followings to avoid authentication error:

- Press your finger evenly to maximize the input area. If we say the weakest push as 0%, and the strongest push as 100%, apply 50~70% of force.



- Make sure that the core of the fingerprint is at the center. In general, the core of the fingerprint is on the same line as the lunula of the fingernail. So locate the lunula of the fingernail at the center of the fingerprint input window.



> ⚠ The recognition performance of the fingerprint recognition device largely depends on the skill of the user. Follow the fingerprint input method described above to improve recognition performance.

## 1.3 Authentication types

With the NITGEN access control system, you can use fingerprints, passwords, and RF cards (optional) for authentication. Depending on customer environment, you can use one of the following authentication types as you need.

### ■ Fingerprint authentication

Use fingerprints to validate access authentication with the following types:

- 1:1 authentication

In this mode, you should input ID first and then your fingerprint. The enrolled fingerprint corresponding to the ID will be compared to the entered fingerprint on a 1:1 basis. The 1:1 authentication type takes a short time regardless of the number of users. There is no need to make any special settings in the system. After entering the ID, enter the fingerprint to perform authentication.

- 1:N authentication

In this mode, you need to enter only fingerprint without ID. Though the authentication procedure is simple, this method will take a little longer than the 1:1 authentication if there are many users. There is no need to make any special settings in the system.

- Short ID (SID) authentication

The user ID can be 4 - 15 digits long depending on the initial setting. This method simplifies ID input procedure. Instead of entering the entire registered ID, you can enter only the first part of the ID for authentication. For example, if the user ID is 1234567, enter 12 only and then the fingerprint. Then the system will perform 1:N authentication for all IDs that start with 12xxxxx. There is no need to make any special settings in the system.

- Group authentication

For group authentication, you can specify a group ID of 1 - 4 digits long for each user group. You will enter a group ID and a fingerprint for authentication. For example, you can use the unit number for public housing like an apartment as a group ID. You can specify a group ID when you register a user. Unlike other methods, **you must enter the group ID, and then press F1 before entering the fingerprint** to perform group authentication.

■ **Password authentication**

A password of 4 - 8 digits long is used to validate access authentication. You can use this method in such a special case as when the fingerprints are damaged.

■ **RF card authentication (optional)**

The RF card of a user is used to identify the user. The card number must be registered into the system to use the card.

# Chapter 2 Installation

## ■ Preparation before installation

1. Fingerprint sensor (USB Type)

To authenticate manager's fingerprint or register user's fingerprint on a server or client PC with the program, NITGEN fingerprint sensor and driver (Easy Installation v.1.32 or later) must be installed.
For more information on how to install, please refer to the enclosed manual ("Driver Installation for fingerprint sensor") with the fingerprint sensor product.

Recommended products : MFDU01 and HFDU01

2. Server and client PCs

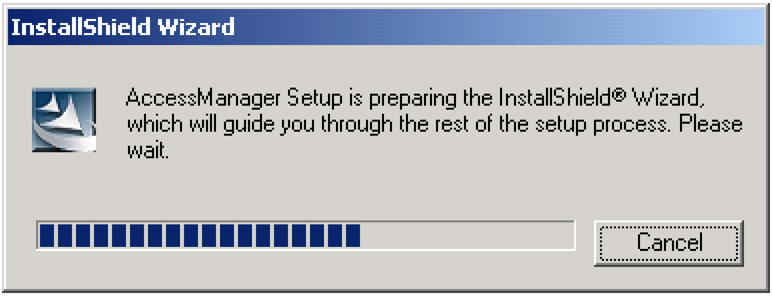
If you have to register a lot of users or manage a lot of te rminals, we recommend installing the program on a stable PC. We also strongly recommend using the server for acce ss controller management only.

3. Network

TCP/IP protocol should be installed on the server and Client PCs. Contact your network administrator to check if a fixed IP address has been assigned to the server PC.

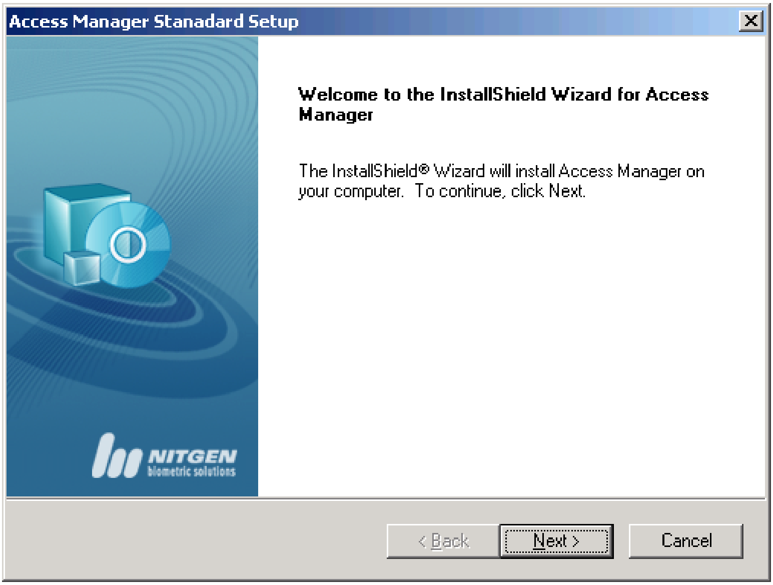
## ■ Installation

Run Setup.exe from the Access Manager folder in the CD, and the installation is proceeding as below:



InstallShield Wizard

AccessManager Setup is preparing the InstallShield® Wizard, which will guide you through the rest of the setup process. Please wait.

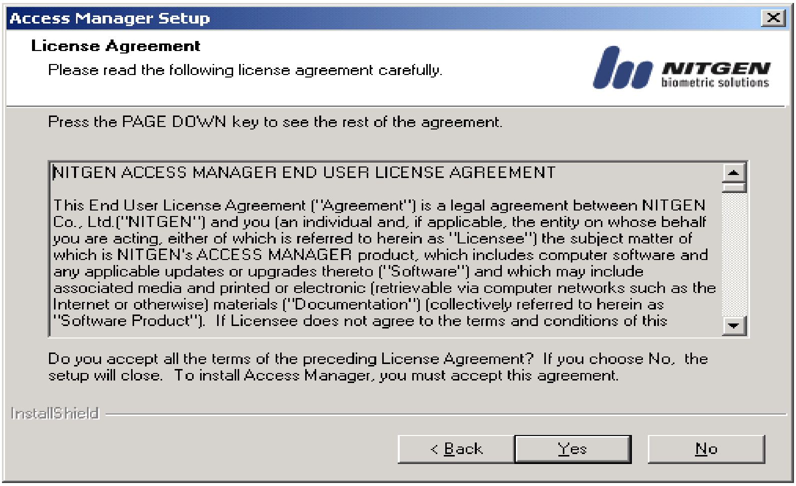


Access Manager Stanadard Setup

**Welcome to the InstallShield Wizard for Access Manager**

The InstallShield® Wizard will install Access Manager on your computer. To continue, click Next.

Click **<NEXT>** to continue the installation.



Access Manager Setup

**License Agreement**

Please read the following license agreement carefully.

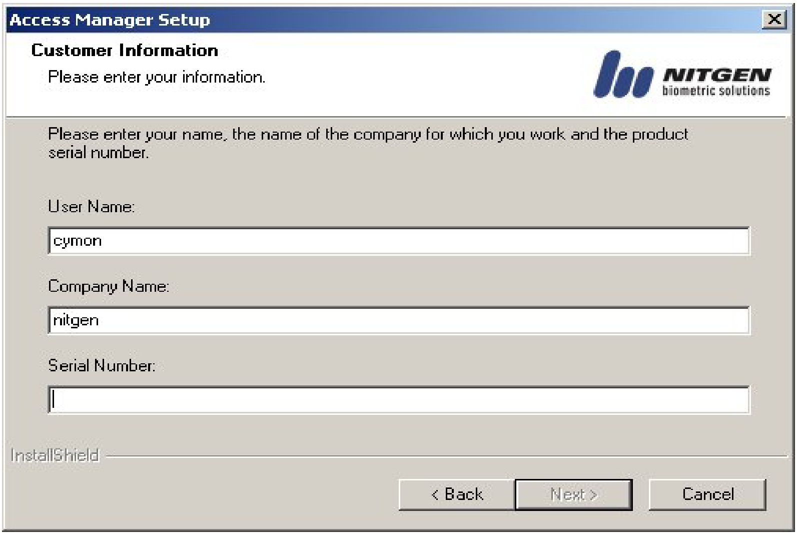
Press the PAGE DOWN key to see the rest of the agreement.

NITGEN ACCESS MANAGER END USER LICENSE AGREEMENT

This End User License Agreement ("Agreement") is a legal agreement between NITGEN Co., Ltd.("NITGEN") and you (an individual and, if applicable, the entity on whose behalf you are acting, either of which is referred to herein as "Licensee") the subject matter of which is NITGEN's ACCESS MANAGER product, which includes computer software and any applicable updates or upgrades thereto ("Software") and which may include associated media and printed or electronic (retrievable via computer networks such as the Internet or otherwise) materials ("Documentation") (collectively referred to herein as "Software Product"). If Licensee does not agree to the terms and conditions of this

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install Access Manager, you must accept this agreement.

Click **<YES>** to accept the license agreement and continue the installation. If you click **<NO>**, the setup will be canceled.



Access Manager Setup

**Customer Information**

Please enter your information.

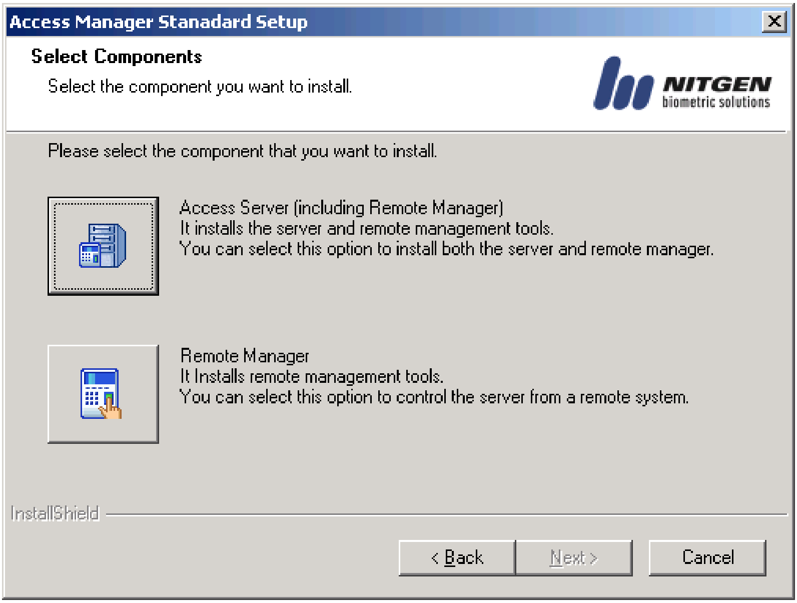
Please enter your name, the name of the company for which you work and the product serial number.

User Name: cymon

Company Name: nitgen

Serial Number:

Enter your information and the Product Serial Number and Click **<NEXT>** to continue the installation.



Access Manager Stanadard Setup

**Select Components**

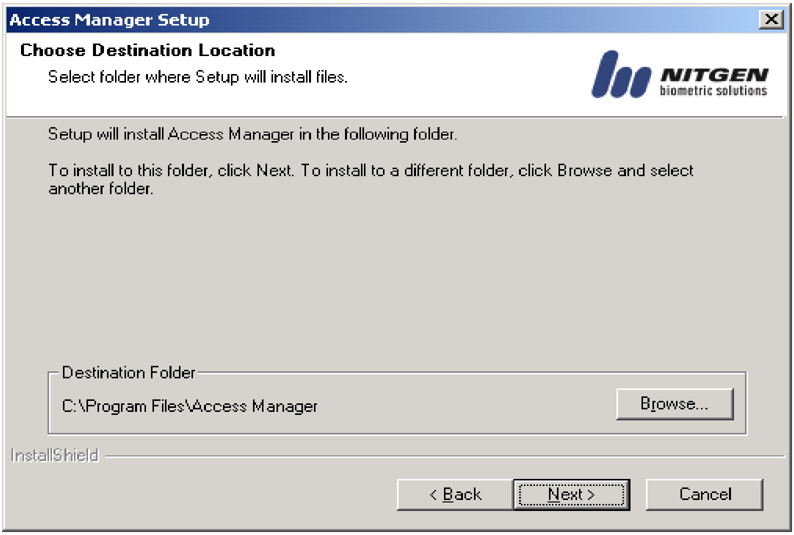
Select the component you want to install.

Please select the component that you want to install.

Access Server (including Remote Manager)
It installs the server and remote management tools.
You can select this option to install both the server and remote manager.

Remote Manager
It Installs remote management tools.
You can select this option to control the server from a remote system.

Click the **<Access Server>** to install the program on the server PC. Or click the **<Remote Manager>** to install it on the remote client PC.



Access Manager Setup

**Choose Destination Location**

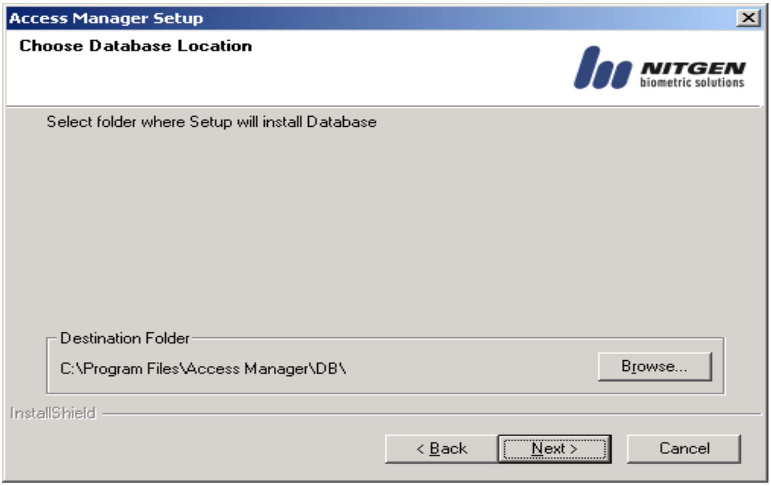
Select folder where Setup will install files.

Setup will install Access Manager in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder
C:\Program Files\Access Manager

If you click **<Next>**, Access Manager will be installed in the default location. To install it in a different location, click **<Browse>** to locate another folder.



Access Manager Setup

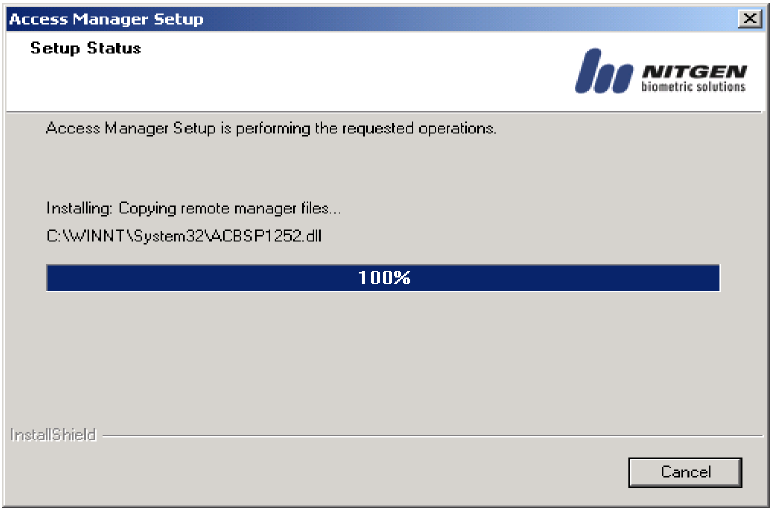
Choose Database Location

Select folder where Setup will install Database

Destination Folder

C:\Program Files\Access Manager\DB\

If you click **<Next>**, the database will be installed in the default location. To install it in a different location, click **<Browse>** to locate another folder.



Access Manager Setup

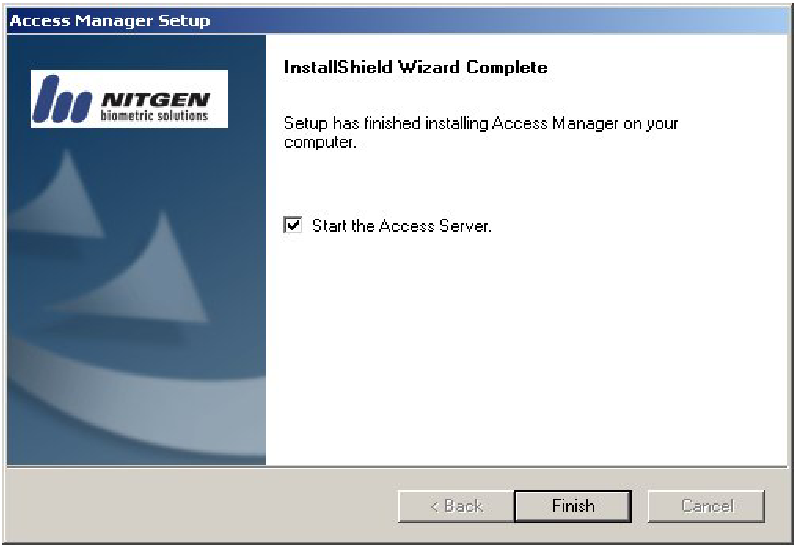
Setup Status

Access Manager Setup is performing the requested operations.

Installing: Copying remote manager files...

C:\WINNT\System32\ACBSP1252.dll

100%



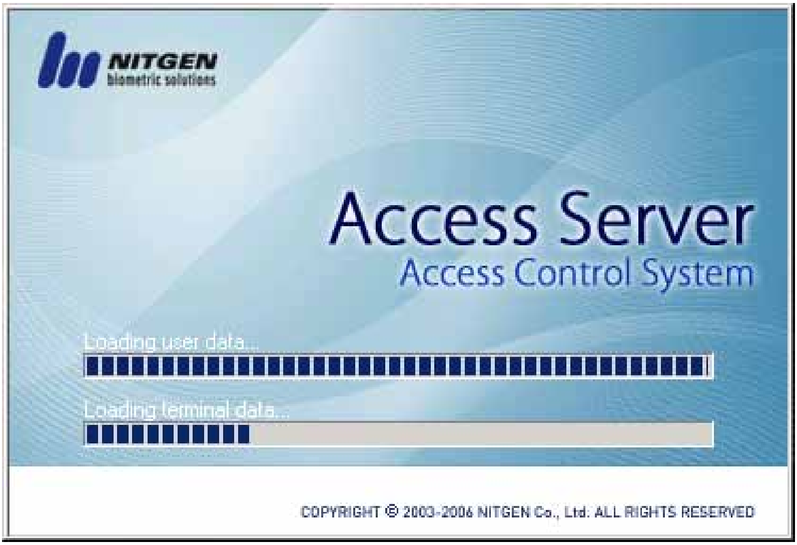
Access Manager Setup

**InstallShield Wizard Complete**

Setup has finished installing Access Manager on your computer.

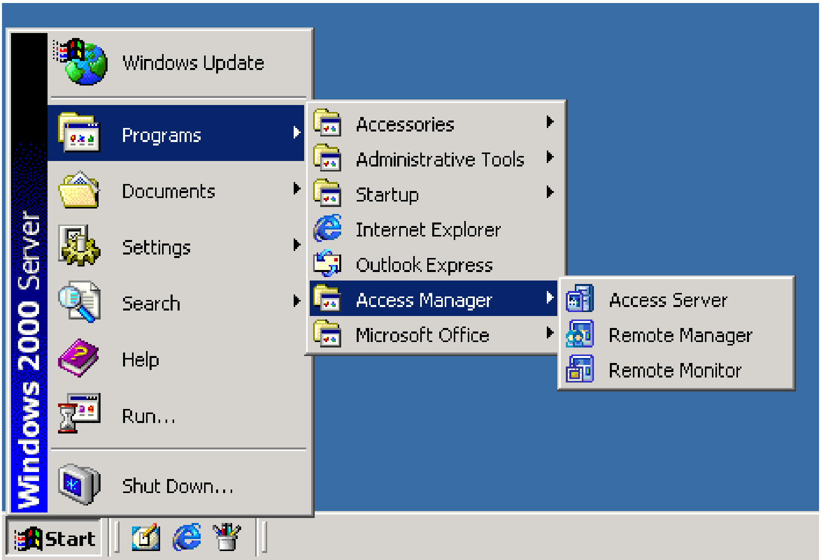
☑ Start the Access Server.

If you click **<Finish>**, the installation will be completed and Access Server will be launched as below:



COPYRIGHT © 2003-2006 NITGEN Co., Ltd. ALL RIGHTS RESERVED

The Access Manager programs are added to the Windows Start menu as below:



# Chapter 3
# Program Introduction

## 3.1 Program overview

Access Manager, the access control program, consists of Access Server (server program), Remote Manager (client program), and Remote Monitor (client program). Remote Manager and Remote Monitor can be installed and used either on a same PC together with Access Server, or on a remote PC on the network.

### ■ Access Server

Access Server communicates with the terminal and the remote manager program. It has user database and event log database, and performs fingerprint authentication in server authentication mode. The manager cannot manage the server directly, but can access and manage it only through Remote Manager and Remote Monitor which are capable of simultaneous access of up to 8.

### ■ Remote Manager

It can be connected to the server to manage database. It can also control and manage the access control terminal connected to the server via the network.

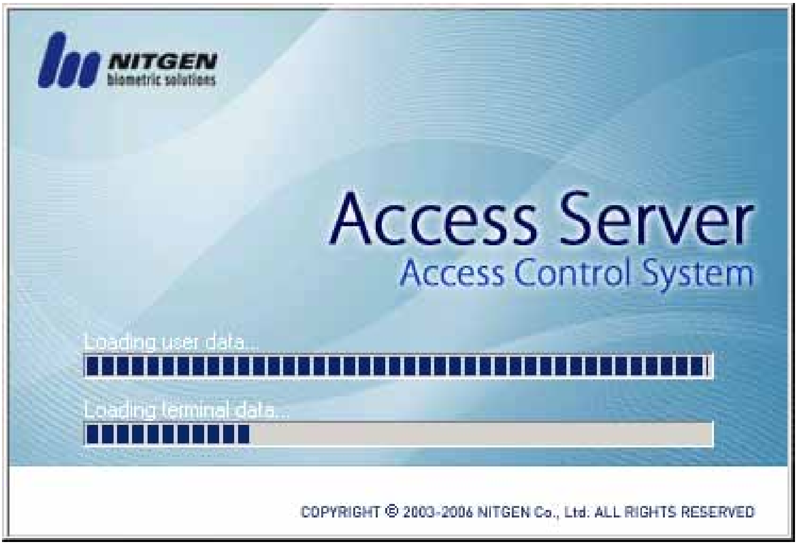
### ■ Remote Monitor

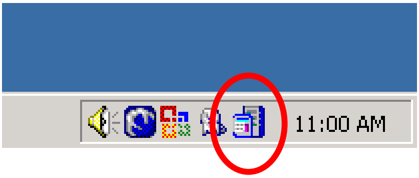
It can be connected to the server to monitor terminal status and event in real-time.

## 3.2 Basic setting and running

### ■ Running and setting of Access Server

When you launch the program, the below screen will appear with the progress bar. After installation is completes, an icon will be displayed in lower right corner of the screen to indicate the server installation status.


NITGEN biometric solutions
Access Server
Access Control System
Loading user data...
Loading terminal data...
COPYRIGHT © 2003-2006 NITGEN Co., Ltd. ALL RIGHTS RESERVED

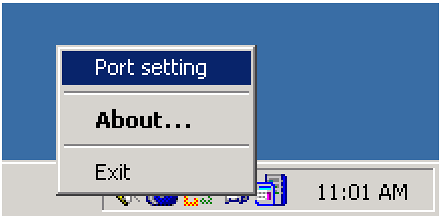


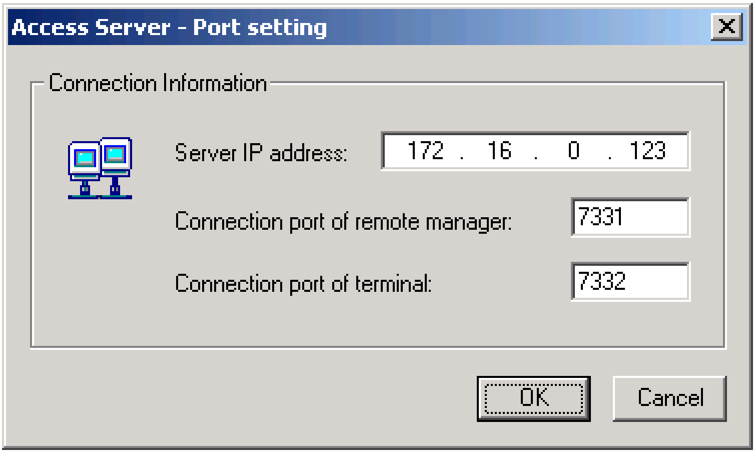
- **Port setting**

Communication port match is required for the remote management programs (Remote Manager and Remote Monitor) or the terminal to communicate with the server (Access Server).

By default, all communication ports are matched. If there is any conflict on server communication port, change it as well as the access port of the remote management program or the terminal.

Right-click the server icon in the lower right corner of the screen and choose **Port setting** to change port.





Access Server - Port setting

Connection Information

Server IP address: 172 . 16 . 0 . 123

Connection port of remote manager: 7331

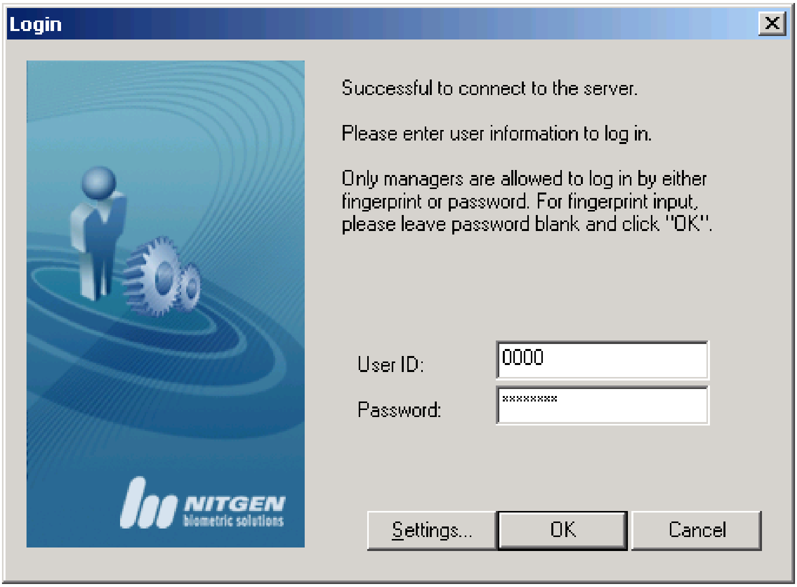
Connection port of terminal: 7332

⚠ The port values displayed on the dialog above, might be different from these of your site.

## ■ Running Remote Manager

⚠ You can use Remote Manager and Remote Monitor only when Access Server is active. Please run Access Server first.

If you install and run Remote Manager in the server PC, you do not need to change network settings. When you run it from a remote location for the first time, you will have to change network settings.



Login

Successful to connect to the server.

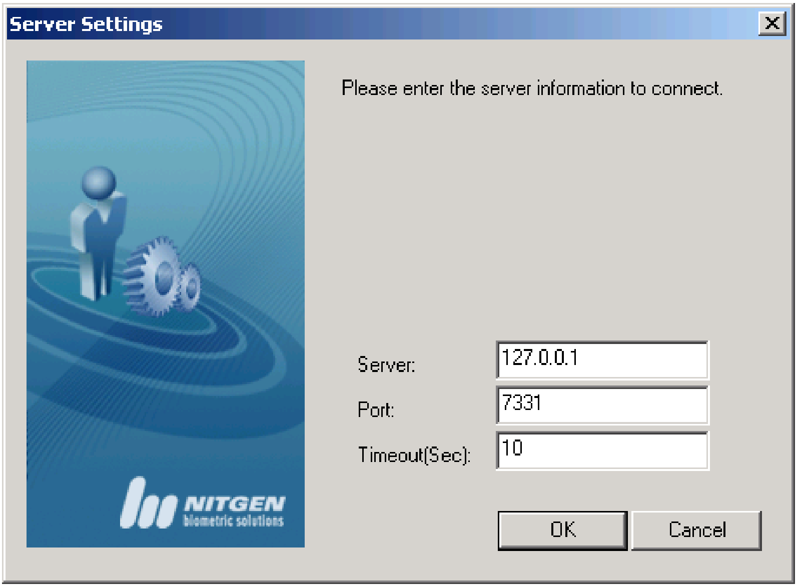
Please enter user information to log in.

Only managers are allowed to log in by either fingerprint or password. For fingerprint input, please leave password blank and click "OK".

User ID: 0000

Password: *********

Click **<Settings...>** and set the network address of the server as follows:



Server Settings

Please enter the server information to connect.

Server: 127.0.0.1

Port: 7331

Timeout(Sec): 10

- Server:

Enter the IP address of the server. The default is 127.0.0.1. If you run Remote Manager in the server PC, use the value.

- Port:

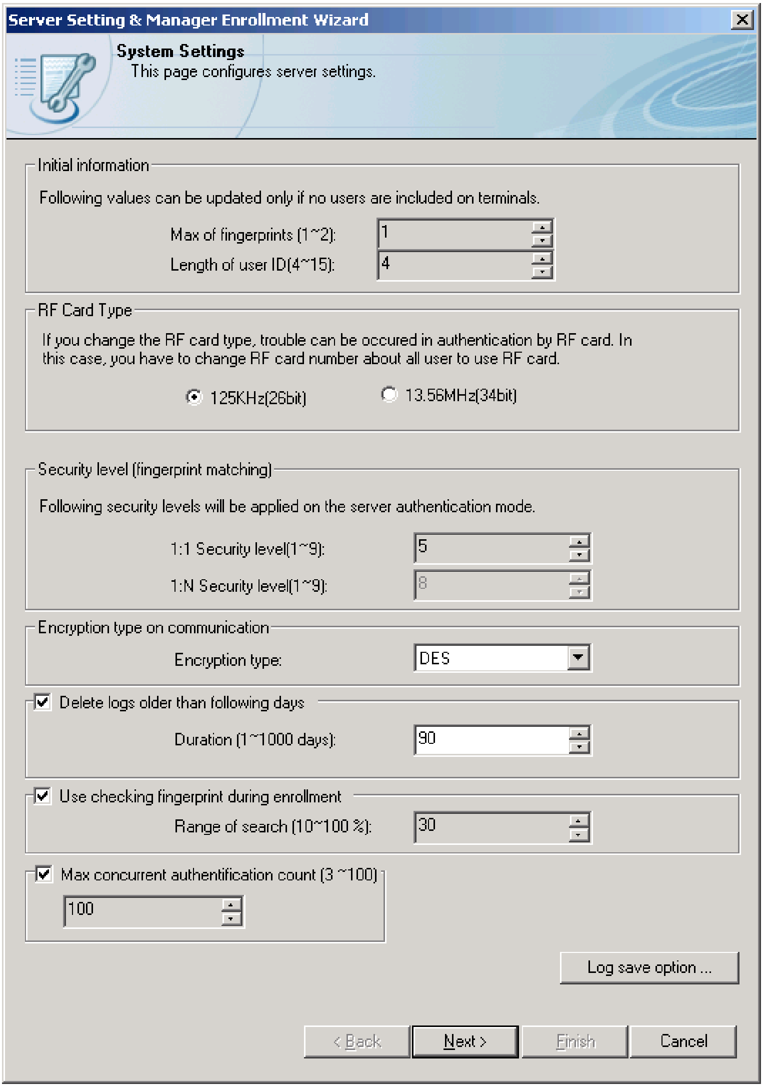
This is a port number for network communication with the server. If there is a conflict, you must change it together with the port value specified in Access Server.

- Timeout (sec):

Enter a timeout value for network connection with the server. Any connection attempt will stop after the specified time.

Click **<OK>** to complete the setting.

If you run Remote Manager for the first time either from the server PC or from a remote PC on the network, the following **Server Setting & Manager Enrollment Wizard** will appear immediately.



Server Setting & Manager Enrollment Wizard

System Settings

This page configures server settings.

Initial information

Following values can be updated only if no users are included on terminals.

Max of fingerprints (1~2): 1

Length of user ID(4~15): 4

RF Card Type

If you change the RF card type, trouble can be occured in authentication by RF card. In this case, you have to change RF card number about all user to use RF card.

● 125KHz(26bit) ○ 13.56MHz(34bit)

Security level (fingerprint matching)

Following security levels will be applied on the server authentication mode.

1:1 Security level(1~9): 5

1:N Security level(1~9): 8

Encryption type on communication

Encryption type: DES

☑ Delete logs older than following days

Duration (1~1000 days): 90

☑ Use checking fingerprint during enrollment

Range of search (10~100 %): 30

☑ Max concurrent authentification count (3 ~100)

100

## ● Initial information

Initial settings are hard to change because of the database structure. So please set them up carefully. But you can increase the value of Max of fingerprints or Length of user ID if you delete all users registered in the terminal.

> ⚠ To decrease the value of Max of fingerprints or Length of user ID, you must delete all users registered in the server.

• Max of fingerprints:
Specify the number of fingerprints that a user can enroll (1~2).

• Length of user ID:
Specify ID length in 4~15 digits.

## ● RF Card Type

When using RF card for user authentication, the RF card type must be selected as the same with one in terminals. Please note that change of this setting requires updating all users' RF input values as well.

- 125 KHz (26bit) – low frequency
- 13.56 MHz (34bit) – high frequency

## ● Security level (fingerprint matching)

Specify security level if you use fingerprint authentication. You can choose a level between 1 and 9. The greater the number is, the higher the security level is. You can specify security levels for 1:1 mode and 1:N mode separately to use the system more efficiently. In general, set the 1:N mode security level higher than the 1:1 mode one.

> ⚠ A high security level may increase the false rejection rate (fail to authenticate the right person) depending on the quality of the fingerprint. In contrast, a low security level may increase the false acceptance rate (allow authentication for the wrong person).

• 1:1 Security level(1~9):
In this mode, ID should be entered first and then fingerprint needs to be entered. The default is 5. The enrolled fingerprint corresponding to the ID will be compared to the entered fingerprint on a 1:1 basis, so you can set lower security level in this mode than in 1:N mode without degrading security.

• 1:N Security level(1~9):
In this mode, you need to enter only fingerprint without ID
The default is 8. (This setting is not updatable.)

- **Encryption type on communication**

Decide whether to encrypt incoming and outgoing content of terminal in network communication.

• Encryption type:
Choose whether to encrypt with DES.

> ⚠ If you use encryption, security and system stability will be enhanced. On the other hand, it will take longer to perform encryption and decryption.

- **Delete logs older than the following days**

You can choose whether to save user access information with period. If the terminal is connected to the network, access information is transferred to the server in real-time, whereas if it is in standalone mode without network connection, information is saved within the terminal.

- **1:N Authentication Time out**

You can set the period of time out for 1:N authentication. The system will search the fingerprint during the certain period of time out. The period range is from 2 seconds up to 9 seconds.

(Default time out value is 3 seconds.)

> ⚠ When the searching is not possible due to undesireably short time out period, you can control the time out value or deactivate this function.

- **Use checking fingerprint during enrollment**

When registering fingerprints for user registration, ‘Use checking fingerprint during enrollment’ prevents overlapping registration of fingerprints if the same or similar fingerprints are registered in the system. By setting a % value, similar fingerprints that may fall within the % range are screened.

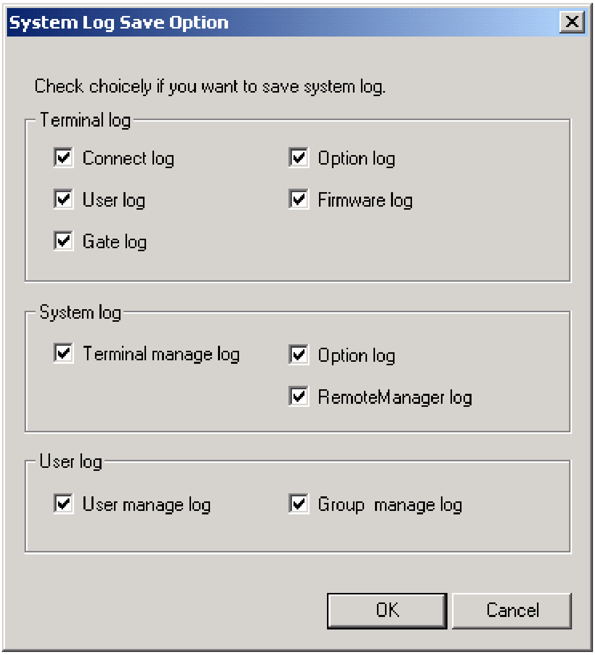
- **Max concurrent authentication count**

The maximum value of concurrent authentication can be set at between 3 to 100 depending on the capability of the system in preparation for the situation in which a multiple number of terminals send signals simultaneously.

## ● Log Save Option

For the system logs only, you can choose to save the logs you want using **System Log Save Option**.

The system logs are diverse and occur frequently. So they need to be saved in consideration of the system capacity. Choose only the logs you need. By default, all are selected.



System Log Save Option

Check choicely if you want to save system log.

Terminal log

☑ Connect log ☑ Option log

☑ User log ☑ Firmware log

☑ Gate log

System log

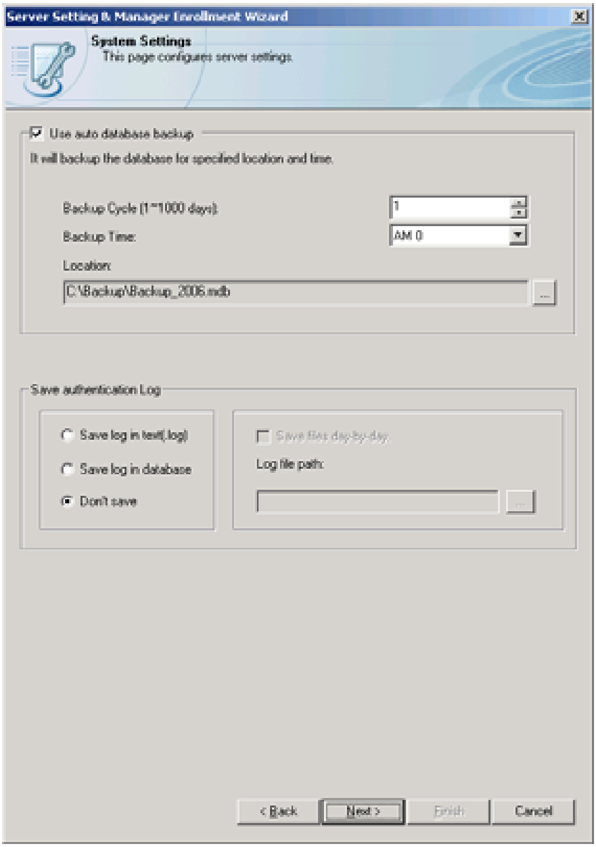
☑ Terminal manage log ☑ Option log

☑ RemoteManager log

User log

☑ User manage log ☑ Group  manage log

Click **<OK>** to continue the initial system setup, and the following window will appear.



Server Setting & Manager Enrollment Wizard

System Settings

This page configures server settings.

☑ Use auto database backup

It will backup the database for specified location and time.

Backup Cycle (1~1000 days): 1

Backup Time: AM 0

Location: C:\Backup\Backup_2006.mdb

Save authentication Log

○ Save log in text(.log)

○ Save log in database

● Don't save

□ Save files day-by-day

Log file path:

In the upper window, **<u>Location can be set only Remote Manager program in the Server PC.</u>**

- Use auto database backup

Choose this option to automatically back up the entire database regularly. You can specify backup cycle (day), backup time, and location.

- Save authentication logs in text

Use this option to save authentication log data as a text file so that it can be used easily in such application as Time & Attendance. The log file is saved separately from log data in the database.

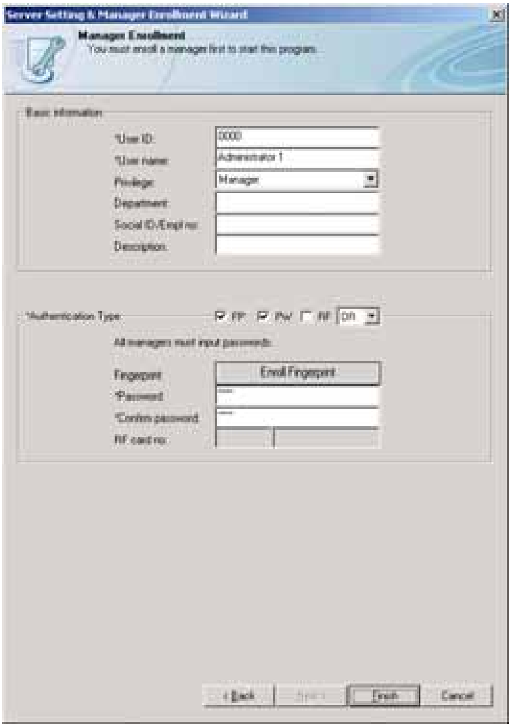
● Save log in text(.log)

If you save the log file by date, the Log file classified by date. (The date is the name of Log file)

● Save log in database

Lod data is saved at original DB in addition to a seperat database. The name of the generated DB is ‘NITGENDBAC_EXT.mdb’, password is ‘123456’. There is only Log data in ‘NITGENDBAC_EXT.mdb’, it can be used for other external application programs.

Click **<Next>** for manager registration, and the following window will appear. You should register at least 1 manager to run the program.



Server Setting & Manager Enrollment Wizard

**Manager Enrollment**
You must enroll a manager first to start the program.

Basic information

| | |
|---|---|
| *User ID: | 0000 |
| *User name: | Administrator 1 |
| Privilege: | Manager |
| Department: | |
| Social ID/Empl no: | |
| Description: | |

*Authentication Type: ☑ FP ☑ PW □ RF OR

All managers must input passwords.

| | |
|---|---|
| Fingerprint: | Enroll Fingerprint |
| *Password: | **** |
| *Confirm password: | **** |
| RF card no: | |

- Basic information

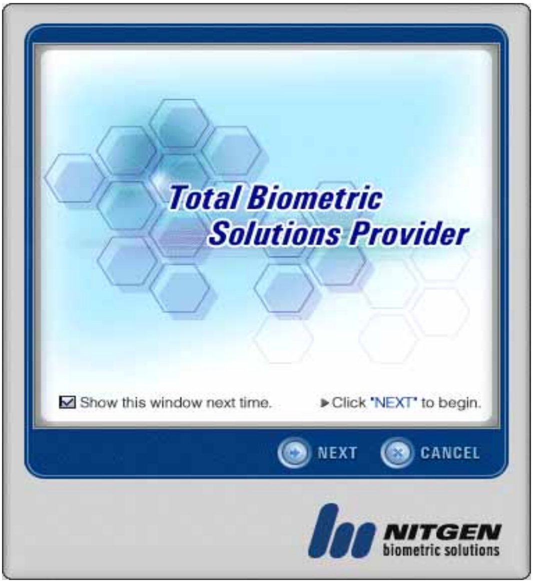
Enter basic manager information. The user ID must be **number** with the digit length of initial setting.

- Authentication Type

You can use fingerprint, password, and RF with AND or OR combination when running application or authenticating terminal access. But RF can be used in terminal access authentication only. For more information on how to use terminal with different authentication types, refer to "***NAC-3000 (or NAC-2500) Terminal User Manual***".

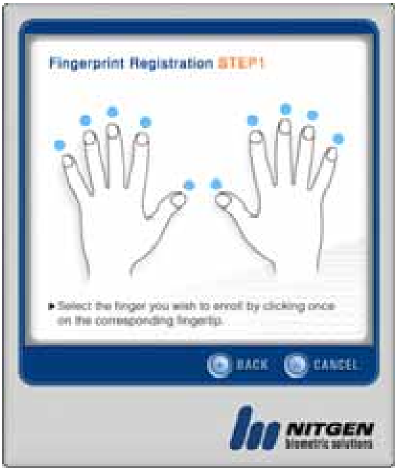
⚠ If you run the program for fingerprint authentication from a server or a remote PC, you need the NITGEN fingerprint recognition device (MFDU01, HFDU01).

Check **FP** and click the **<Enroll Fingerprint>** button to display the following window. If you do not use fingerprint authentication, check **PW** and enter Password ignoring the following procedure.



The above window is the starting place of fingerprint enrollment. Click **<Next>** to continue.

In the below window, check the finger of which fingerprint you want to enroll.

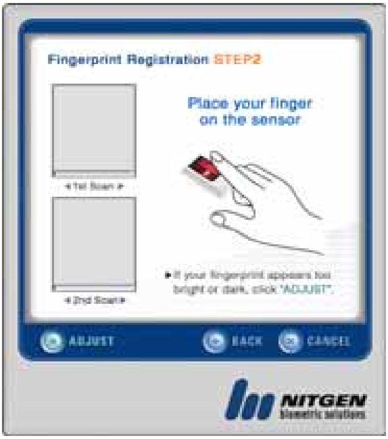


Fingerprint Registration STEP1

▸ Select the finger you wish to enroll by clicking once on the corresponding fingertip.

When you choose a finger, the following window will appear. If you choose two fingers, you should repeat the same registration procedure for the second finger.

If you want to replace an enrolled finger with another, click it again to remove and choose another one.



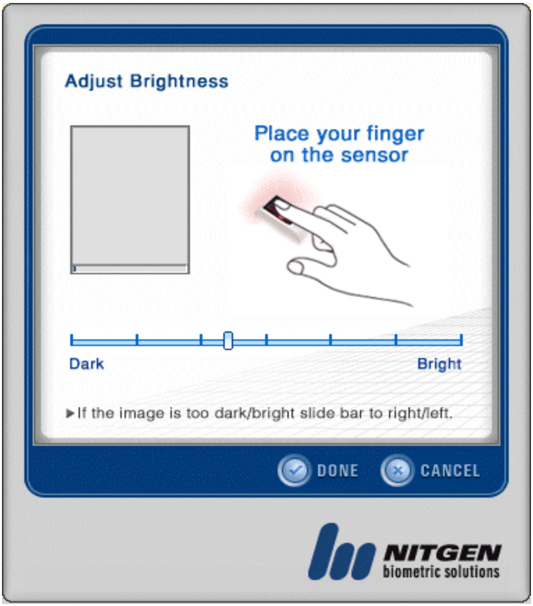
Fingerprint Registration STEP2

Place your finger on the sensor

▸ If your fingerprint appears too bright or dark, click "ADJUST".

If you place the finger you chose in the previous step on the fingerprint recognition sensor, its image will appear in the left image box. Take off your finger and place it on the sensor once again to complete the registration.

If you have problem with fingerprint registration, you can adjust the brightness to optimize the condition. Click **<ADJUST>**, and the following window will appear.



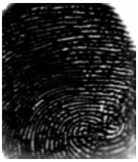
Adjust Brightness

Place your finger on the sensor

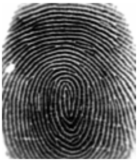
▶If the image is too dark/bright slide bar to right/left.

Place your finger on the fingerprint sensor, and use the slider to adjust the brightness. Make adjustment so that fingerprint image does not look too dark or too dim.

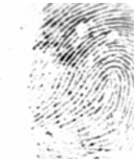
⚠ If your finger is sweaty or wet, the image will look black and dark. And if it is dry, the image will look dim. Make adjustment until you get the normal image as shown below.



Wet fingerprint (x)

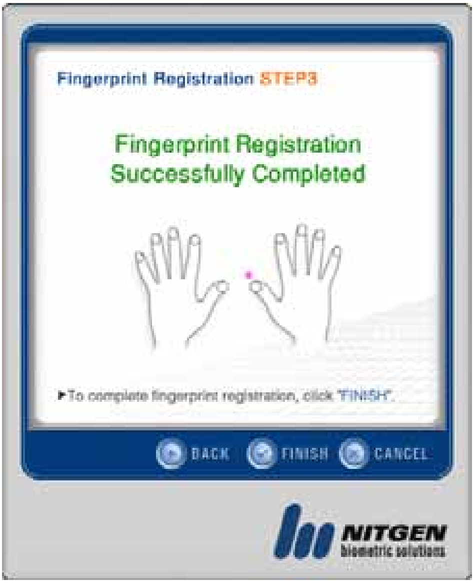


Normal fingerprint (O)



Dry fingerprint (x)

Click **<Done>** button to go back to the previous window. When you complete the registration, the following success message will appear.

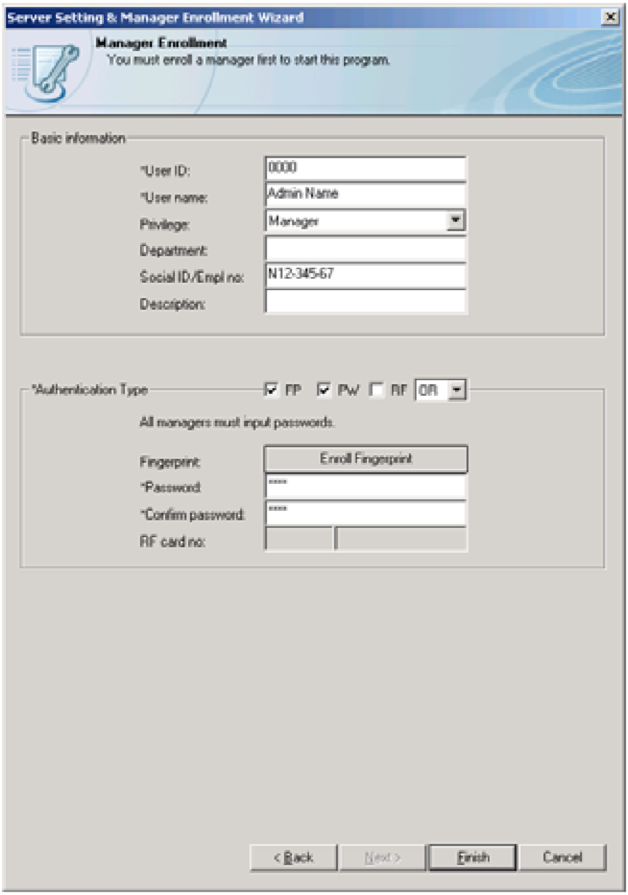


Fingerprint Registration STEP3

Fingerprint Registration Successfully Completed

▸To complete fingerprint registration, click 'FINISH'.

Click **<Done>** button to complete fingerprint registration procedure, and you will go back to the following **Manager Enrollment** window.



Server Setting & Manager Enrollment Wizard

**Manager Enrollment**

You must enroll a manager first to start this program.

Basic information

| | |
|---|---|
| *User ID: | 0000 |
| *User name: | Admin Name |
| Privilege: | Manager |
| Department: | |
| Social ID/Empl no: | N12-345-67 |
| Description: | |

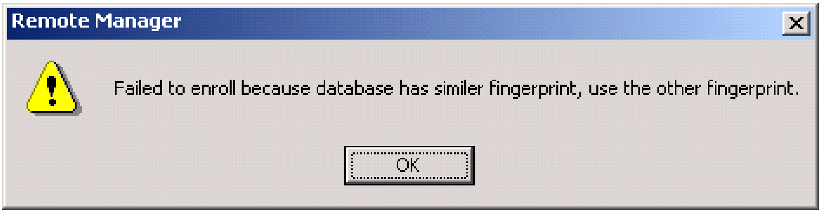
*Authentication Type ☑ FP ☑ PW □ RF OR

All managers must input passwords.

| | |
|---|---|
| Fingerprint: | Enroll Fingerprint |
| *Password: | **** |
| *Confirm password: | **** |
| RF card no: | |

Enter a password and press **<Finish>**, and the main window of Remote Manager will appear.

When you activated the similar fingerprint check function, it will close down the fingerprint registration window if similar or the same fingerprints are about to be registered with the following error message.



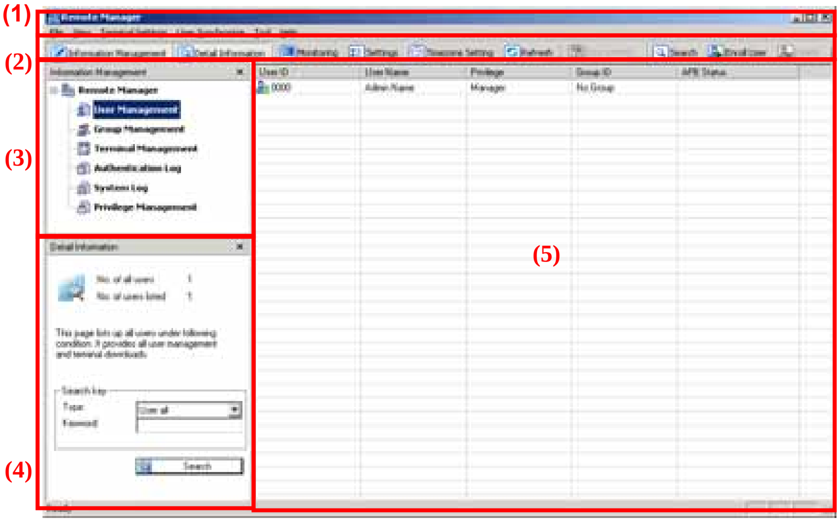
Remote Manager

Failed to enroll because database has similer fingerprint, use the other fingerprint.

In this case, you have to use a different fingerprint to continue the registration process.

## 3.3 About menu

### ■ Screen configuration



| User ID | User Name | Privilege | Group ID | APB Status |
|---|---|---|---|---|
| 0000 | Admin Name | Manager | No Group | |

No. of all users 1
No. of users listed 1

This page lists up all users under following condition. It provides all user management and terminal downloads.

Search key
Type: User all
Keyword:

### (1) Menu bar

This is the main menu of Remote Manager.

- **File:**

It provides such basic features as register, delete, search, view properties, reconnect terminal, and close. Depending on the submenu in the **Information Management window** or selected list, you'll see different active/inactive commands.

- **View:**

You can configure the screen as you need. You can show or hide the **Information Management** and **Detail Information** windows. Depending on the selected item in the **Information Management** menu, the **List window** will be changed.

- **Terminal Settings:**

You can change the settings for several terminals at once.

- **User Synchronize:**

If the user information on the server is different from the one in the terminal, you can synchronize them. If you select any terminal in the List window, List up Users and Synchronize All Data will be activated.

- **Tool:**

You can do configurations for terminal monitoring, server options and Anti Pass Back.

If you select Detail Information from Information Management Window, excel printing settings will be activated.

- **Help:**

You can get the software version.

### (2) Toolbar

Frequently used features are gathered in one place so that you can access them easily. Depending on the submenu you select in the Information Management window, its configuration will be changed.

- Information Management:

Show or hide the Information Management window.

- Detail Information:

Show or hide the Detail Information window.

- Monitoring:

Start remote management monitoring.

- Settings:

Set the program options.

● Timezone Setting:

You can set up the timezone in many different ways: by hour, day of the week, holiday, etc.

Also, You can keep the door opening always.

● Refresh:

Update the list if there's any change.

● Gate Control:

Managers have the right to open gates.

This option is to activate or deactivate the gate control function. After activating this option, gate controlling menus will be enabled, **<Gate Control>** on the Remote Manager toolbar.

⚠ The 'Use timezone' of terminal is true, you can't use this function.
If you are going to use this function, you should change the 'Use timezone' setting with 'false'.

### (3) Information Management window

You can select the management menu items. If you choose any menu item, related data will appear in the List window on the right. Right-click any menu item to show submenu.

### (4) Detail Information window

When you select a menu item in the Information Management window, statistical information on the corresponding data list will appear. In addition, you can use the Search window to find any necessary information with search conditions.

### (5) List window

This window shows data list and related information of the menu item selected in the Information Management window. Double-click any list item to see detailed information. You can use the <Shift> or <Ctrl> key to select several items at once.

⚠ Keyboard shortcuts will help you to use the menu and commands more easily. Press a shortcut key of a menu while holding down the <Alt> key on the keyboard. If the menu is open, you can simply press the corresponding shortcut key of any submenu or command to select it.

- Description of icons

| Terminal status | | Description |
|---|---|---|
| NAC-3000 | NAC-2500 | |
| ▦ | ▦ | The terminal is in normal status. |
| # | # | The terminal has a synchronization error. |
| ? | ? | The terminal is connected, but not registered. |
| X | X | The terminal is not connected. |
| ! | ! | The terminal has other errors. |

| User status | Description |
|---|---|
| 👤 | Normal user |
| 👤🔒 | Program manager |
| 👤🔒 | Power User |
| 👤 | Guest |
| 👤⌛ | Expired user |
| 👥 | Group |

| Log status | Description |
|---|---|
| ✓ | Authentication succeeded |
| ✗ | Authentication failed |
| 👤✓ | System log of user information changes such as registration and deletion |
| ✓ | System log of terminal setting change |
| 🖥✓ | System log of program execution and setting change |

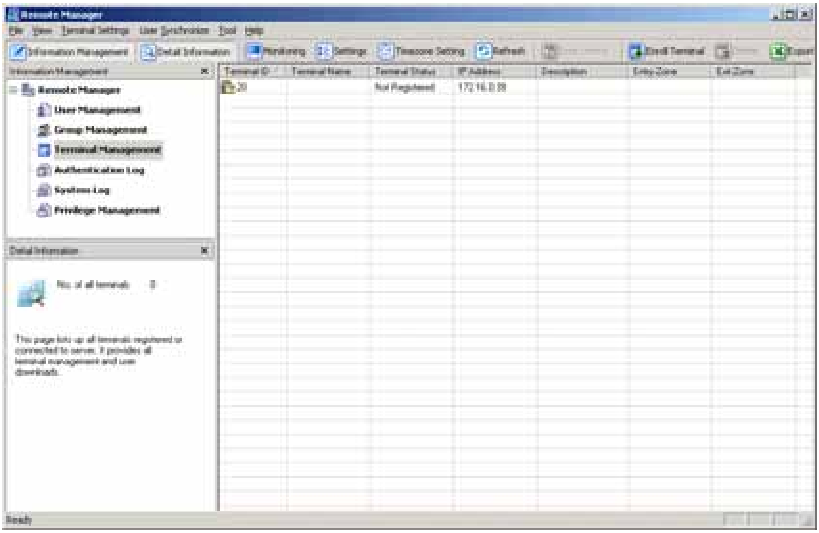
# Chapter 4
# How to Use the Program

## 4.1 Terminal Management

You can select **Terminal** in the **Information Management window** to do the necessary job on terminal.

### ■ Register a new terminal

If network setting is complete in a terminal with physical network connection, you can see the terminal in the program. You can register a new terminal as follows:



| Terminal ID | Terminal Name | Terminal Status | IP Address | Description | Entry Zone | Exit Zone |
|---|---|---|---|---|---|---|
| 20 | | Not Registered | 172.16.0.39 | | | |

No. of all terminals 0

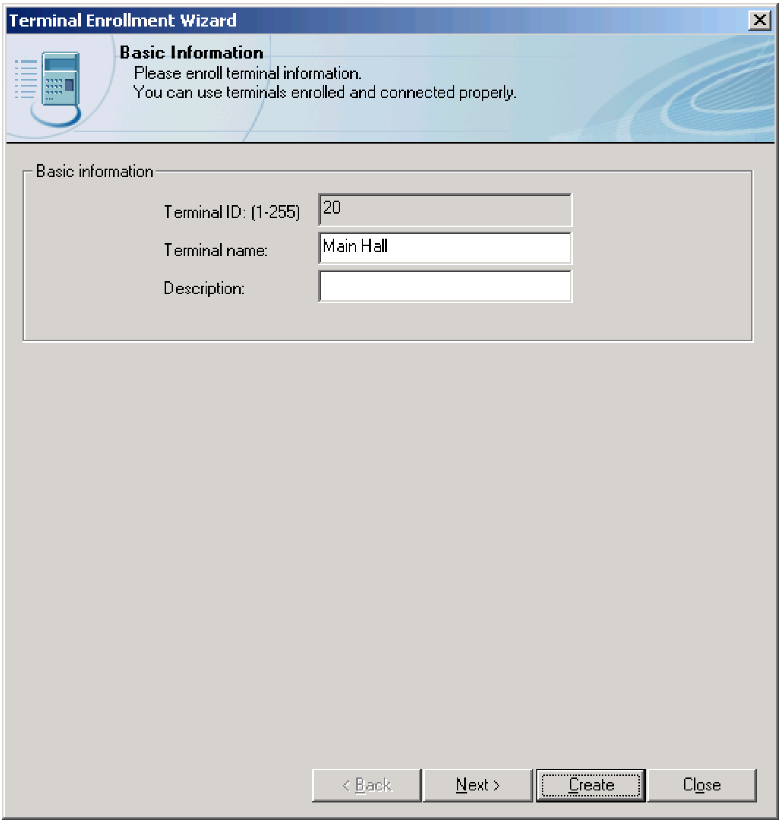
This page lists up all terminals registered or connected to server. It provides all terminal management and user downloads.

(1) Select **Terminal Management** in the **Information Management window.**

(2) Double-click a terminal in the **List window** on the right, or right-click a terminal to select **Enroll Terminal** from the submenu.

(3) The **Terminal Enrollment Wizard** window will appear as below. The terminal ID is already entered.

⚠ Right-click **Terminal Management** or use the **Enroll Terminal** button from the **Toolbar** to register a new terminal. Unlike selecting a terminal in the **List window**, however, the terminal ID is not entered in this case.



Please enroll terminal information.
You can use terminals enrolled and connected properly.

Basic information

Terminal ID: (1-255) 20

Terminal name: Main Hall

Description:

Enter the terminal name and description, and proceed with the buttons below.

**<Next>:** Proceed to the next step to add users to or delete users from the terminal.

**<Create>:** Register another terminal.

**<Close>:** Cancel what you've done and exit the wizard window.

## ■ Delete Terminal

You can delete a terminal as follows:

(1) Select **Terminal Management** in the **Information Management window.**

(2) Right-click a terminal in the **List window** and select **Delete** from the submenu, or use the **<Delete>** key on the keyboard to delete it. You can use the **<Shift>** or **<Ctrl>** key to delete several terminals at once.

> ⚠ After deleting a terminal, When you re-register it, you should add users to the terminal again.

## ■ Terminal Properties

You can check and change the basic information of registered terminals.

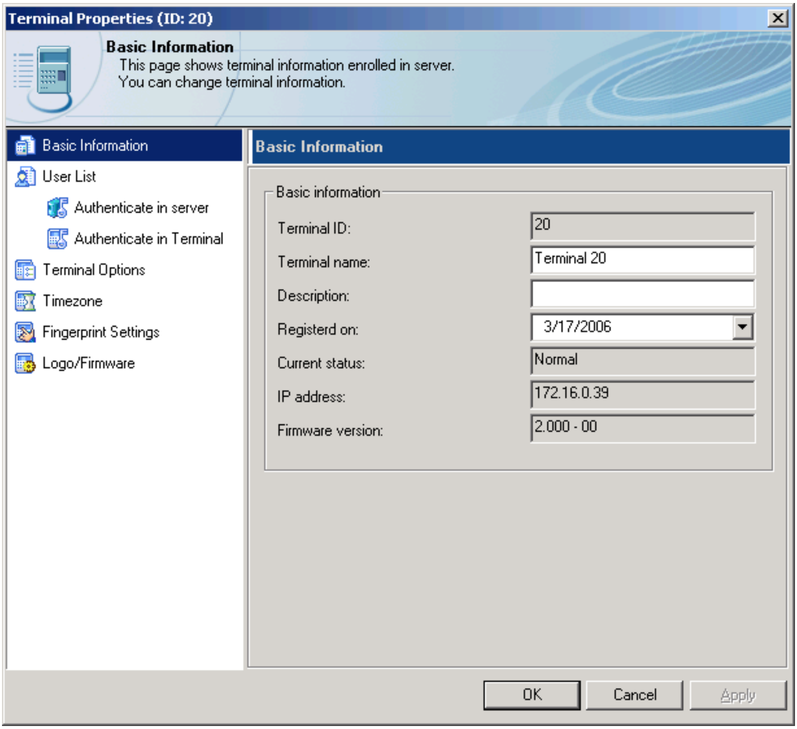
(1) Select **Terminal Management** in the **Information Management window.**

(2) Right-click a terminal in the **List window** and choose **Properties** from the submenu.

(3) When the **Terminal Properties** window is open, related information will be displayed according to the submenu you select on the left, and you can change this information.

## ● Basic Information.

You can check basic terminal information and modify name and description in this window.



Terminal Properties (ID: 20)

Basic Information

This page shows terminal information enrolled in server.
You can change terminal information.

Basic Information

Basic information

Terminal ID: 20

Terminal name: Terminal 20

Description:

Registerd on: 3/17/2006

Current status: Normal

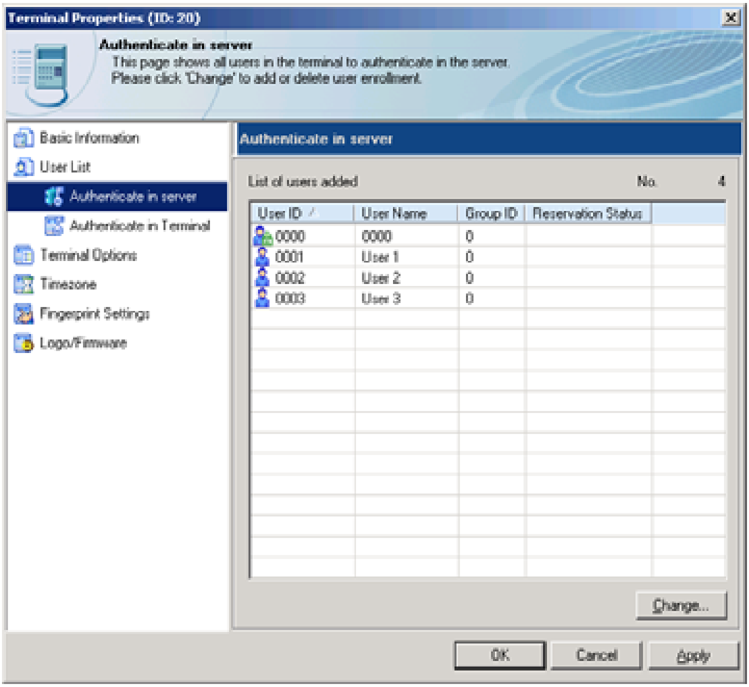
IP address: 172.16.0.39

Firmware version: 2.000 - 00

You can check basic terminal information and modify name and description in this window.

- **Authenticate in server**

You can check the list of terminals authenticated by the server and can add or delete users by clicking **<Change>**. User information will not be stored in the terminal but the relevant user can still use the system through authentication. 1:N authentication is not possible and therefore you must type in user ID and use fingerprint.



Terminal Properties (ID: 20)

Authenticate in server

This page shows all users in the terminal to authenticate in the server.
Please click 'Change' to add or delete user enrollment.

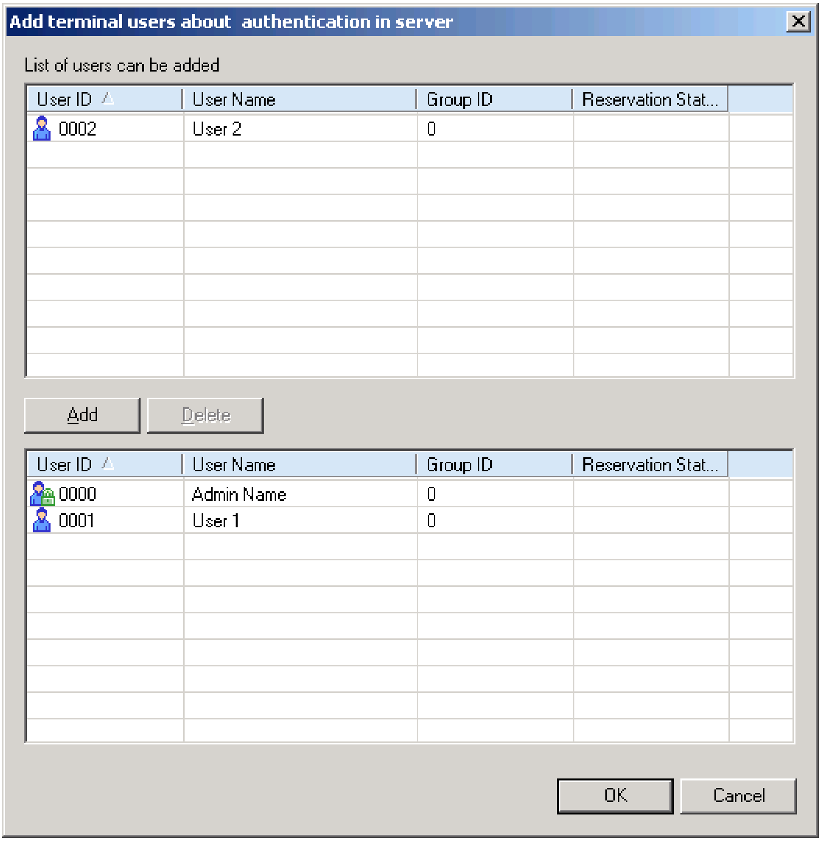
Authenticate in server

List of users added     No.  4

| User ID | User Name | Group ID | Reservation Status |
|---|---|---|---|
| 0000 | 0000 | 0 | |
| 0001 | User 1 | 0 | |
| 0002 | User 2 | 0 | |
| 0003 | User 3 | 0 | |

⚠ Adding or deleting users in a terminal may take from several seconds to tens of minutes depending on the number of users.

Server authenticated user should type in user ID and use fingerprint when authenticated in the terminal.



Add terminal users about  authentication in server

List of users can be added

| User ID | User Name | Group ID | Reservation Stat... |
|---|---|---|---|
| 0002 | User 2 | 0 | |

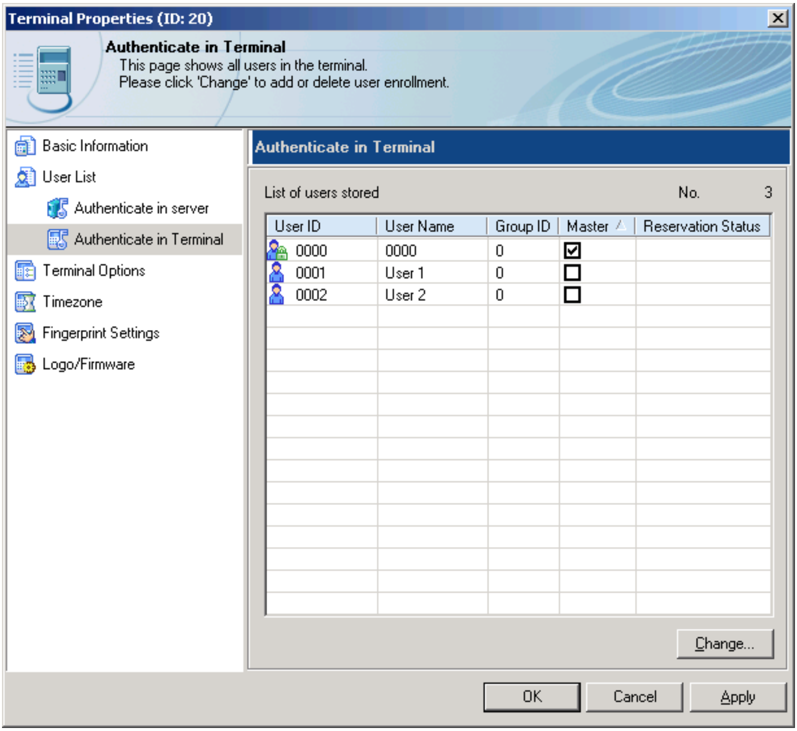
| User ID | User Name | Group ID | Reservation Stat... |
|---|---|---|---|
| 0000 | Admin Name | 0 | |
| 0001 | User 1 | 0 | |

⚠ "Reservation" can be used to reserve user download operations into terminals on specified date.

⚠ All reserved users are not available for authentication until they are downloaded into terminals. The reservation date must be later than the current date.

## ● Authenticate in terminal

This is the list of users stored in the terminal and the relevant users will be authorized in terminal. You can check the user list registered in the terminal. To add or delete users, click **<Change>**.



Terminal Properties (ID: 20)

**Authenticate in Terminal**

This page shows all users in the terminal.
Please click 'Change' to add or delete user enrollment.

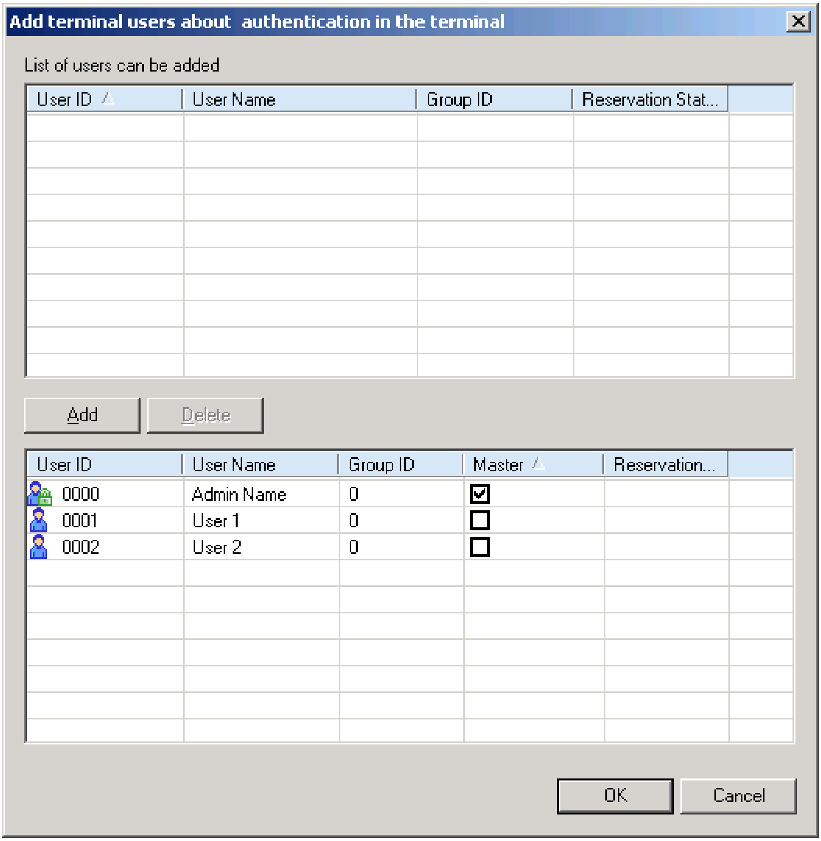
Authenticate in Terminal

List of users stored    No. 3

| User ID | User Name | Group ID | Master | Reservation Status |
|---|---|---|---|---|
| 0000 | 0000 | 0 | ☑ | |
| 0001 | User 1 | 0 | □ | |
| 0002 | User 2 | 0 | □ | |

⚠ Adding or deleting users in a terminal may take from several seconds to tens of minutes depending on the number of users. Please take note that the terminal doesn't work while adding or deleting users.

⚠ Users authorized in terminal can be authorized only with fingerprint. (1:N authenication possible)



Add terminal users about authentication in the terminal

List of users can be added

| User ID | User Name | Group ID | Reservation Stat... |
|---|---|---|---|

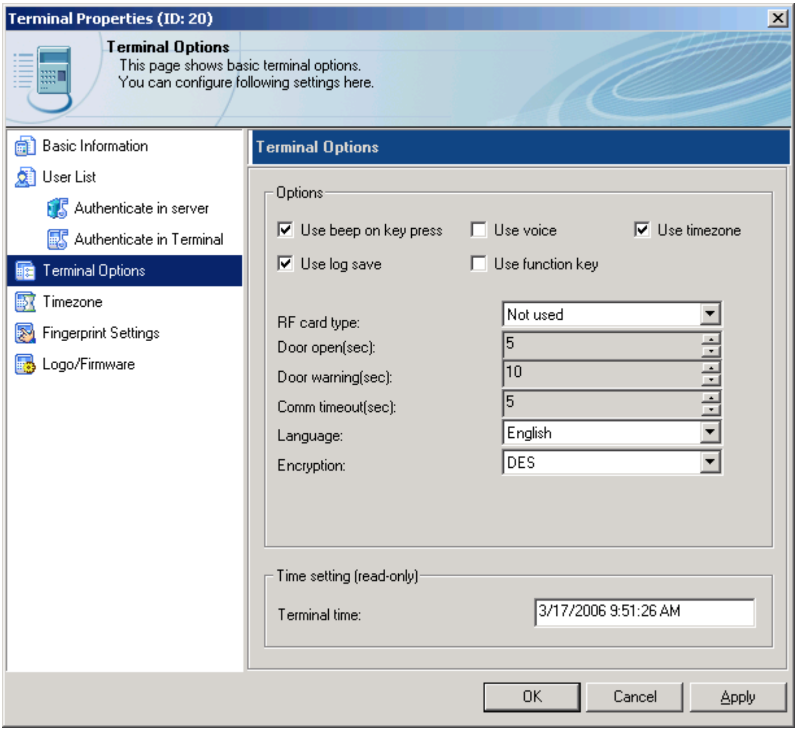
| User ID | User Name | Group ID | Master | Reservation... |
|---|---|---|---|---|
| 0000 | Admin Name | 0 | ☑ | |
| 0001 | User 1 | 0 | □ | |
| 0002 | User 2 | 0 | □ | |

⚠ One or more Master should be registered to the each terminal, Master can change all terminal settings.

⚠ “Reservation” cannot be the master of a terminal.

## Terminal Options

You can set or modify terminal options and time as follows:



Terminal Properties (ID: 20)

**Terminal Options**
This page shows basic terminal options.
You can configure following settings here.

Terminal Options

Options

☑ Use beep on key press ☐ Use voice ☑ Use timezone
☑ Use log save ☐ Use function key

RF card type: Not used
Door open(sec): 5
Door warning(sec): 10
Comm timeout(sec): 5
Language: English
Encryption: DES

Time setting (read-only)

Terminal time: 3/17/2006 9:51:26 AM

- Use Beep on Key Press

Decide whether use Button Beep.

- Use voice

Provide voice instruction on how to use the terminal for fingerprint authentication.

- Use timezone

Each terminal should determine whether to use a timezone function or not. If this option is not selected, the terminal cannot

run timezone-related functions.
This option is not applicable to NAC-3000.

- Use log save

Save user access information. If the terminal is connected to the network, event information is sent to the server in real-time, whereas in standalone mode without network connection, information is saved within the terminal.

> ⚠ You can save up to 3,000 latest events in NAC-3000 terminal.
>
> ⚠ In case NAC-2500, you can save up to 1,500 latest events in a terminal.

- RF Card Type

When using RF card for user authentication, the RF card type must be selected as the same with one in terminals.

> ⚠ RF Card is an optional part of terminals. You cannot use this option for any terminial with no RF module attached.

- Use function key

Choose this option to make the terminal's function keys (F1 ~ F4) available in such application as Time & Attendance. But you cannot use group authentication while it is active.

- Door open (sec)

You can specify how long the door will be open after user authentication is validated. You can specify between 1 and 20.

- Door warning (sec)

It gives an alarm if the door is still open after the specified time elapses. If the alarm sounds, check why the door is not closed and take necessary steps to make sure that the door closes normally. Specify a value between 1 and 20, but it should be greater than the door open time.

⚠ **Door open** and **Door warning** may not work in some types of doors.

- Comm timeout (sec)

When the terminal communicates with the server via the network, it will be assumed that the network connection is disabled if there is no response within the specified time. You can specify a value between 2 and 20. If the network environment is not stable, start with 5 seconds and then increase the value gradually.

- Language

Select the language (Korean or English) of LCD display.

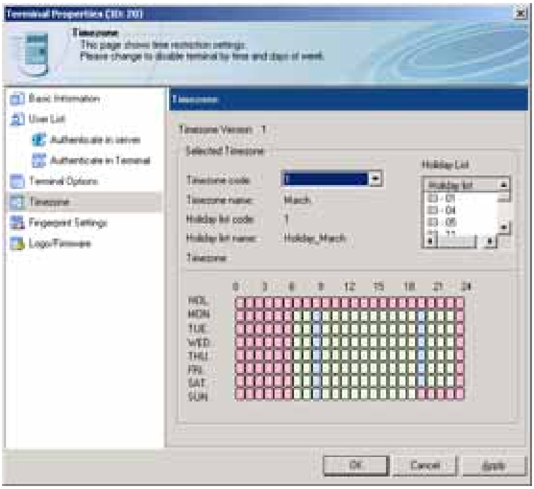
- Encryption

Choose whether to use DES encryption type for the contents transferred via the network.

- Time setting (read-only)

It displays the current time of the terminal. You cannot change the time in this window.

- Timezone



Timezone
This page shows time restriction settings.
Please change to disable terminal by time and days of week.

Timezone Version: 1

Selected Timezone

Timezone code: 1
Timezone name: March
Holiday list code: 1
Holiday list name: Holiday_March

It shows the currently selected timezone.

To change the timezone, select Timezone Setting from the toolbar. For more information, refer to 4.6 Timezone Setting later in this manual.

NAC-3000 Terminal don’t has the time that a entry is always opened.

- Timezone Version

If you change the timezone in the Timezone Setting window, the version increases. This version is used to synchronize the information saved in the terminal and the server.

- Selected Timezone

From the terminal, you must select at least one of the maximum 16 timezones set up in the Timezone Setting window. If you select a timezone from the Timezone code combo box, the information on the selected timezone will be displayed in a table form, and the terminal operates with this timezone.

With regard to the holiday list, you can select one holiday code for one timezone. You can also change it in the Timezone Setting window.

⚠ **How to read the timezone table**

There are horizontal axis marked with 0, 3, 6, 9…, and vertical axis marked with HOL, MON…in the timezone table.

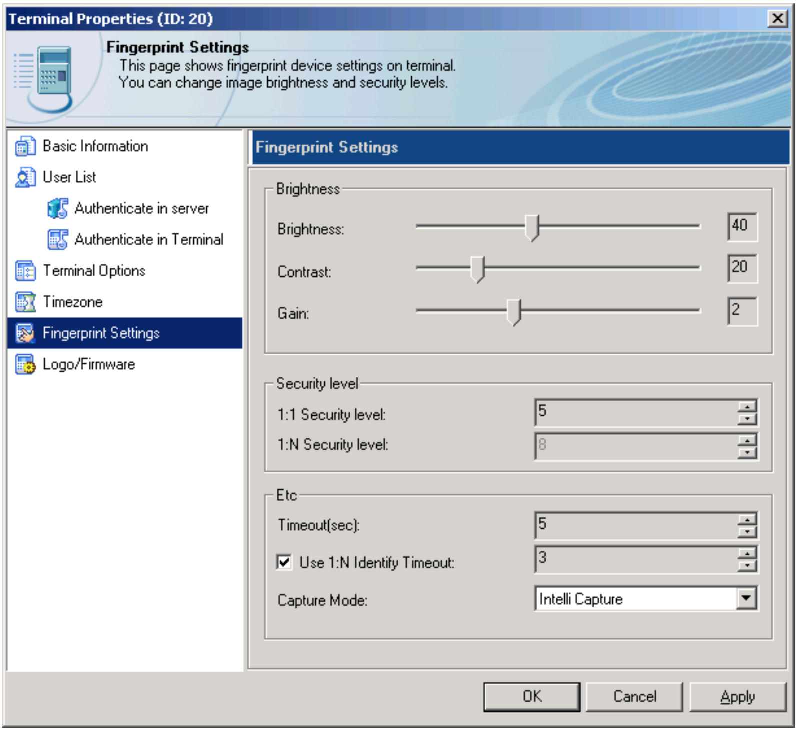
Green is the time for “permit the access”. Red is the time for “deny the access”. Blue is the time for “always opened the door”.

If a holiday is selected and the date of the holiday is specified, it will work first regardless of the day of the week.

EX1. As any access is denied for the entire 24 hours for holiday list, terminals set for common users cannot have an access on a specific date under holiday list.

EX2. For weekday, doors are set open from 8:00 AM to 9:00 AM, and users can have an access without authentication.

## ● Fingerprint settings



Terminal Properties (ID: 20)

**Fingerprint Settings**

This page shows fingerprint device settings on terminal.
You can change image brightness and security levels.

Fingerprint Settings

Brightness

Brightness: 40

Contrast: 20

Gain: 2

Security level

1:1 Security level: 5

1:N Security level: 8

Etc

Timeout(sec): 5

☑ Use 1:N Identify Timeout: 3

Capture Mode: Intelli Capture

• Brightness

You can obtain a clear fingerprint image by adjusting the fingerprint settings. The defaults of Brightness, Contrast and Gain are 40, 20 and 2 respectively.

⚠ These values can largely affect the fingerprint recognition performance because they are very sensitive. So it is highly recommended that default values be used without any modification if possible.

⚠ If the recognition performance is decreased because it is very dry (i.e. in winter), adjust Brightness between 20 and 30 (recommendation: 20).

⚠ If the recognition performance is decreased because it is very wet (i.e. in summer), adjust Brightness between 50 and 80 (recommendation: 60).

- Security level

You can choose a level between 1 and 9. The greater the number is, the higher the security level is. The default value of 1:1 Security level is 5 and that of 1:N Security level is 8. The default is 8. (This setting is not updatable.)

For more information, please refer to **3.2 Basic setting and running.**

- Etc

(1) Timeout (sec)

You can set the timeout of fingerprint input within the range of 1 and 30 seconds. The terminal waits for fingerprint input during the specified seconds. After that time, the LED will be turned off. The default is 5 seconds.

(2) 1:N Authentication Time out

You can set the period of time out for 1:N authentication. The system will search the fingerprint during the certain period of time. The period range is from 2 seconds up to 9 seconds.
(Default time out value is 3 seconds)

(3) CAPTURE MODE

► Latent

To prevent any possible False Recognition by fingerprint latent which remain on the surface of sensor formed by dirt and sebum.

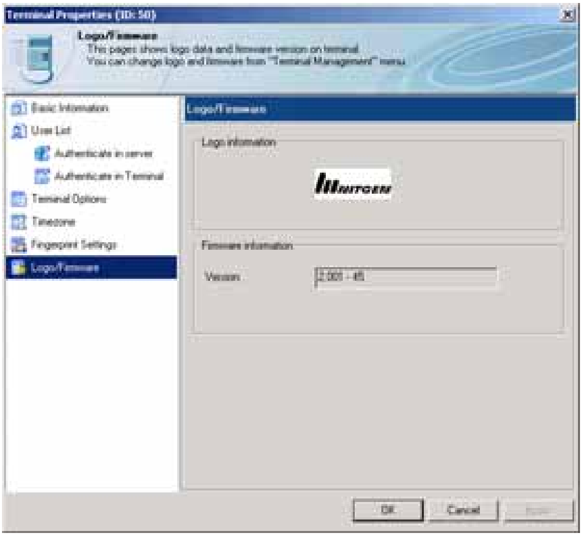
► Intelli Capture

To optimise the brightness of the fingerprint image captured from extremely dry or wet finger.

Intelli Capture Mode contains Latent mode.

⚠ This feature can increase security but it may slow down authentication time. So if high level of security is required, you can use this feature. But you'd better not use this feature in an environment where convenience and quickness are more important (i.e. when used for Time & Attendance).

- **Logo/Firmware**



Terminal Properties (ID: 50)

Logo/Firmware

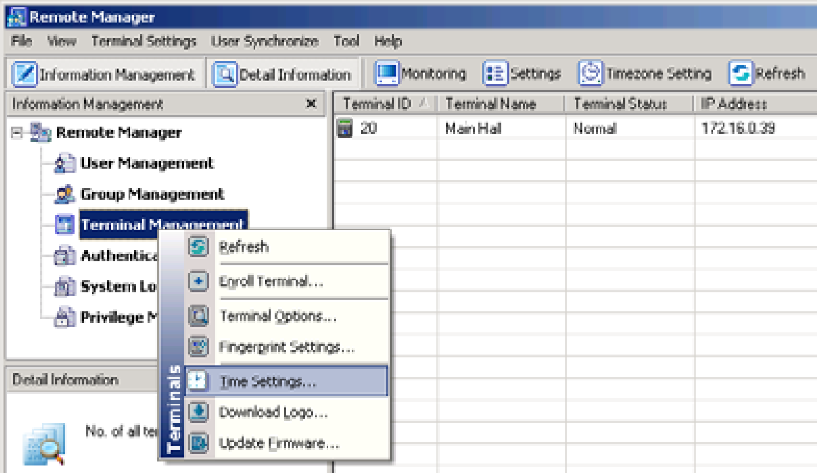
This pages shows logo data and firmware version on terminal

You can change logo and firmware from "Terminal Management" menu

Version: 2.001 - 45

You can check the logo and firmware version stored in the terminal from the above window.

## ■ Terminal Time Settings



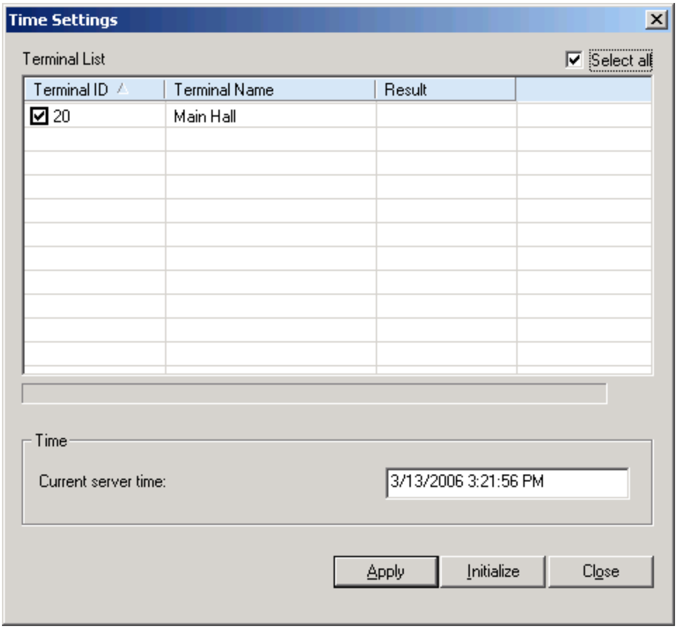
| Terminal ID | Terminal Name | Terminal Status | IP Address |
|---|---|---|---|
| 20 | Main Hall | Normal | 172.16.0.39 |

When the terminal is connected to the server, the terminal time is automatically synchronized, but you can synchronize the time manually.

Right-click **Terminal** in the **Information Management window** and choose **Time Settings** from the submenu, and the **Time Settings** window will appear.

Alternatively, right-click a terminal in the **List window** and select **Time Settings** from the submenu.

Select one or more terminals and click **<Apply>** to synchronize with the server time.



Time Settings

Terminal List ☑ Select all

| Terminal ID | Terminal Name | Result |
|---|---|---|
| ☑ 20 | Main Hall | |

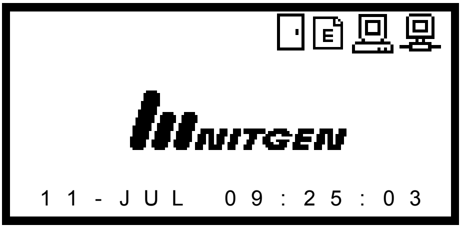
Time

Current server time: 3/13/2006 3:21:56 PM

## ■ Download Logo

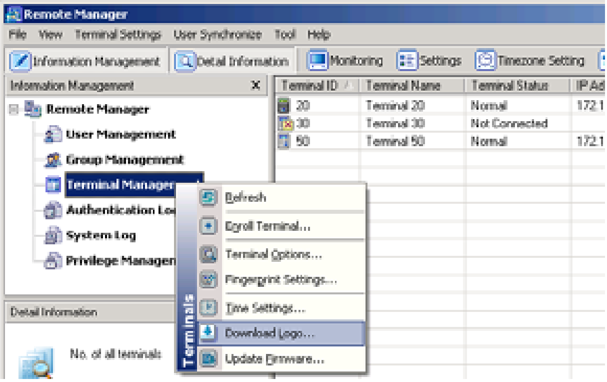
As shown in the below terminal LCD screen, you can register a new logo or change the logo for a terminal.

NAC-3000 terminal only support this function.



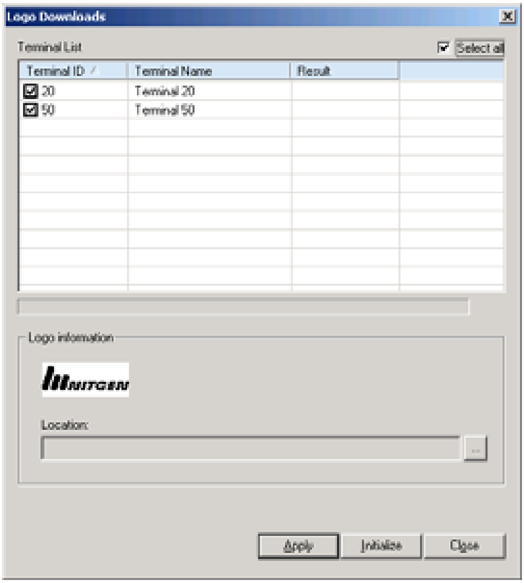
Right-click **Terminal Management** in the **Information Management window** and choose **Download Logo** from the submenu, and the **Logo Downloads** window will appear.

Alternatively, right-click a terminal in the **List window** and select **Download Logo** from the submenu.



| Terminal ID | Terminal Name | Terminal Status | IP Ad |
|---|---|---|---|
| 20 | Terminal 20 | Normal | 172.1 |
| 30 | Terminal 30 | Not Connected | |
| 50 | Terminal 50 | Normal | 172.1 |

In the following window, click **<…>** to locate the logo file you want to download to a terminal. Then select the terminal and click **<Apply>**. You can use only a black and white bitmap image ( 2color, *.bmp) with the size of 80 x 32 pixels as a log file.



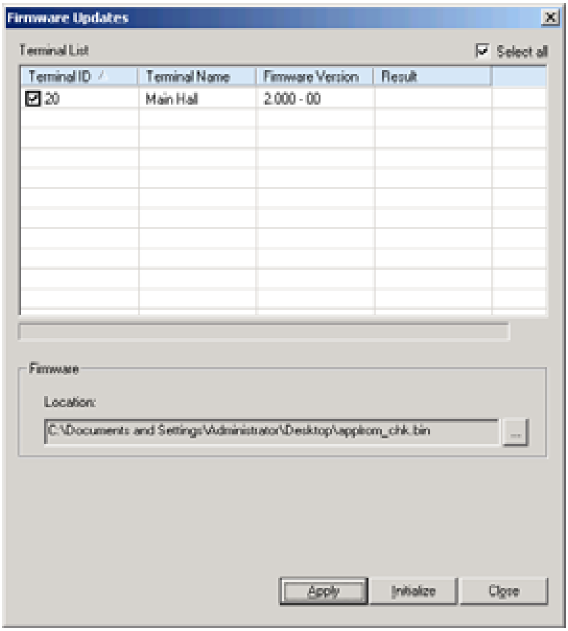
| Terminal ID | Terminal Name | Result |
|---|---|---|
| ☑ 20 | Terminal 20 | |
| ☑ 50 | Terminal 50 | |

## ■ Update Firmware

You can use this feature to update firmware of terminal.

Right-click **Terminal Management** in the **Information Management window** and choose **Update Firmware** from the submenu, and the following **Firmware Updates** window will appear.

Alternatively, right-click a terminal in the **List window** and select **Update Firmware** from the submenu.



Firmware Updates

Terminal List

☑ Select all

| Terminal ID | Terminal Name | Firmware Version | Result |
|---|---|---|---|
| ☑ 20 | Main Hall | 2.000 - 00 | |

Firmware

Location: C:\Documents and Settings\Administrator\Desktop\applrom_chk.bin

Click **<...>** to locate the firmware file you want to download to a terminal. Then select the terminal and click **<Apply>**.

## ■ Terminal Options

Right-click **Terminal Management** in the **Information Management window** and select **Terminal Options** from the submenu, or select **Terminal Settings > Terminal Options** from the **Menu bar** to change the settings of several terminals at once.

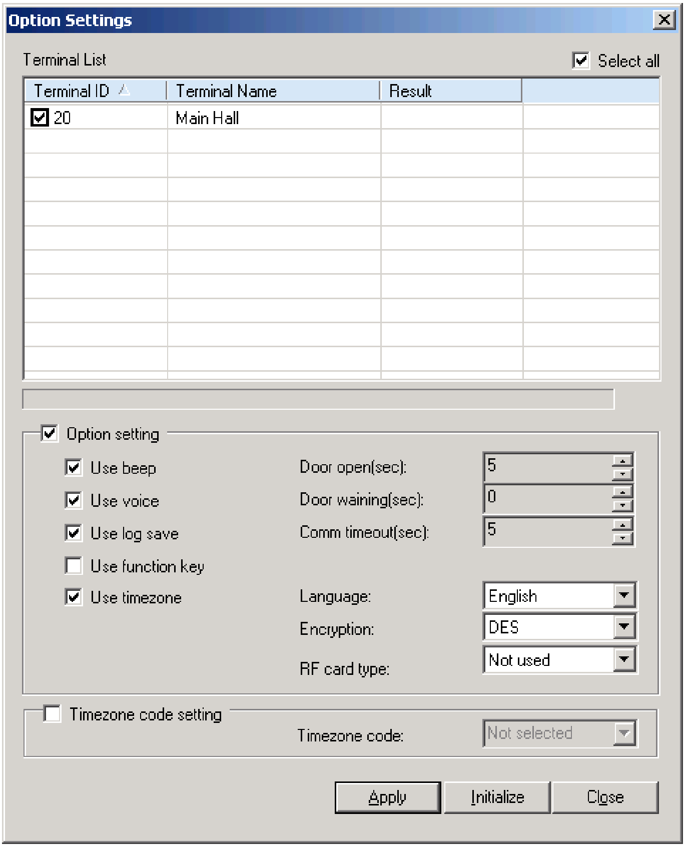
Select each terminal and make necessary changes, and then click **<Apply>** to change the settings at once.

● Option setting check boxes

If you select an option setting, you can change its value.

● Timezone code check box

If you select **Timezone code setting**, you can change the timezone code.



Option Settings

Terminal List ☑ Select all

| Terminal ID | Terminal Name | Result |
|---|---|---|
| ☑ 20 | Main Hall | |

☑ Option setting

☑ Use beep
☑ Use voice
☑ Use log save
□ Use function key
☑ Use timezone

Door open(sec): 5
Door waining(sec): 0
Comm timeout(sec): 5
Language: English
Encryption: DES
RF card type: Not used

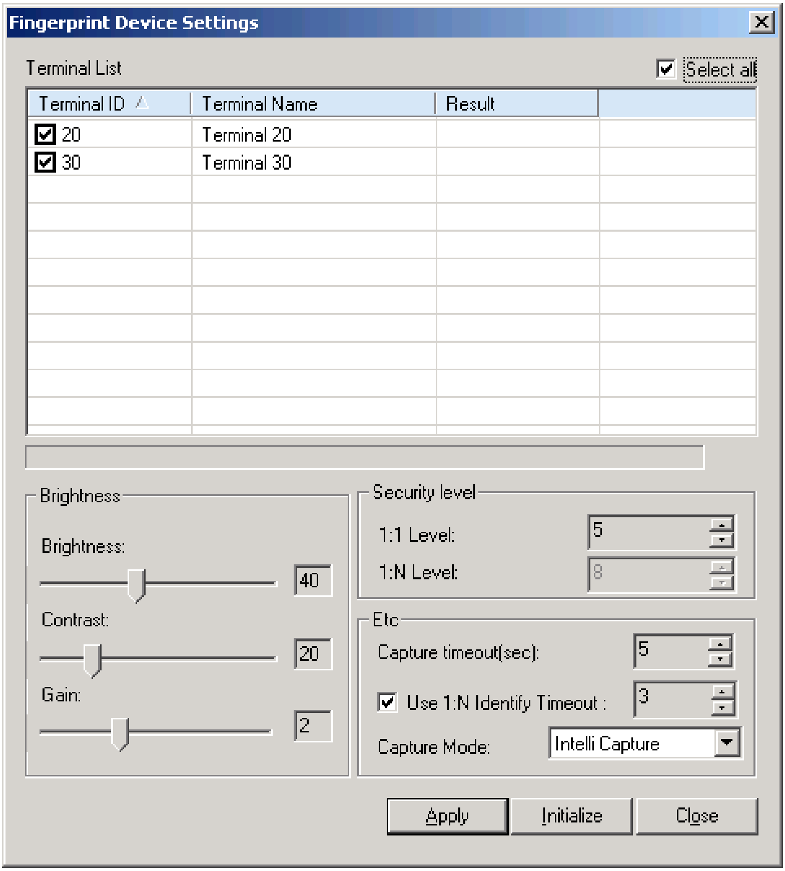
□ Timezone code setting

Timezone code: Not selected

## ■ Fingerprint Device Settings

Right-click **Terminal Management** in the **Information Management window** and choose **Fingerprint Settings** from the submenu, or select **Terminal Settings > Fingerprint Settings** from the menu bar to change the setting of several terminals at once.

Select each terminal and make necessary changes, and then click **<Apply>** to change the settings at once.



Fingerprint Device Settings

Terminal List ☑ Select all

| Terminal ID | Terminal Name | Result |
|---|---|---|
| ☑ 20 | Terminal 20 | |
| ☑ 30 | Terminal 30 | |

Brightness

Brightness: 40

Contrast: 20

Gain: 2

Security level

1:1 Level: 5

1:N Level: 8

Etc

Capture timeout(sec): 5

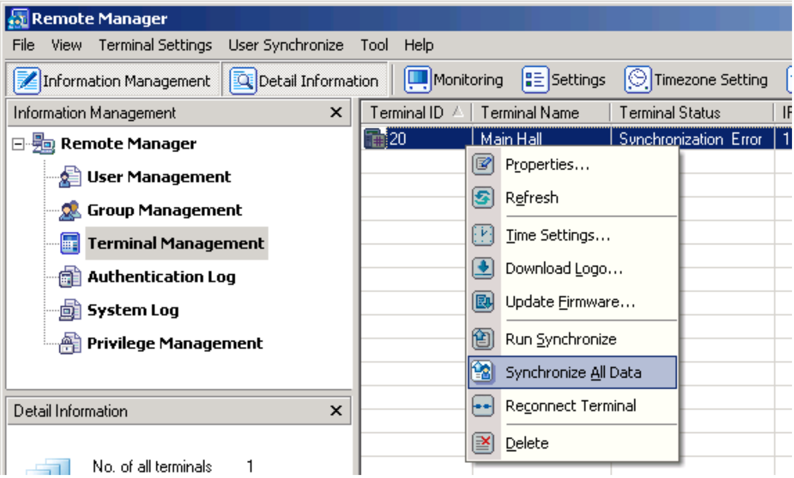
☑ Use 1:N Identify Timeout : 3

Capture Mode: Intelli Capture

## ■ Synchronization

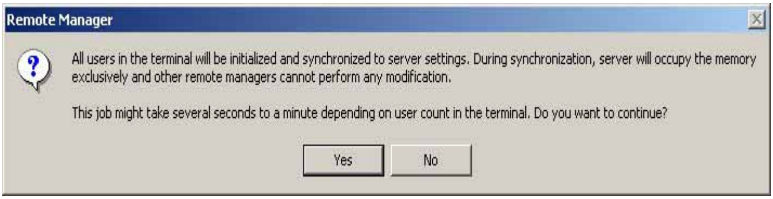
If user group and timezone information are changed in the server, the corresponding information in the terminal will be changed as well. If the information saved in the server and terminal doesn't match each other because of network or other problems, schronization errors may occur. The role of synchronization is to correct those errors according to the information in the server. If a synchronization error occurs, you can see such status as below on the screen.

Right-click on the terminal that has a synchronization error, and you can see **Run Synchronize** or **Synchronize All Data** from the menu.



| Terminal ID | Terminal Name | Terminal Status | IP |
|---|---|---|---|
| 20 | Main Hall | Synchronization Error | 1 |

Click **Synchronize All Data** to synchronize all user data between the server and the selected terminal. Doing this will solve all synchronization errors including ID length mismatch or registered fingerprint count mismatch.

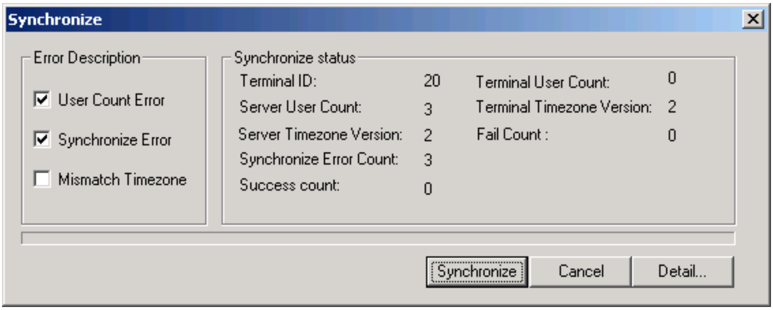


Remote Manager

All users in the terminal will be initialized and synchronized to server settings. During synchronization, server will occupy the memory exclusively and other remote managers cannot perform any modification.

This job might take several seconds to a minute depending on user count in the terminal. Do you want to continue?

If you select **Run Synchronize**, the following screen will appear.



Synchronize

Error Description

☑ User Count Error

☑ Synchronize Error

☐ Mismatch Timezone

Synchronize status

|  |  |  |  |
|---|---|---|---|
| Terminal ID: | 20 | Terminal User Count: | 0 |
| Server User Count: | 3 | Terminal Timezone Version: | 2 |
| Server Timezone Version: | 2 | Fail Count : | 0 |
| Synchronize Error Count: | 3 |  |  |
| Success count: | 0 |  |  |

● **Error Description**

There are three types of synchronization errors.

**User Count Error**: It occurs when the user count in the terminal is different from that in the server.

**Synchronize Error**: It occurs when the user information in the terminal is different from that in the server.

**Mismatch Timezone**: It occurs when the timezone setting in the terminal is different from that in the server.

**Error Description** shows which of these errors occur.

● **Synchronize status**

Brief information is provided so that you can identify the cause of the error.

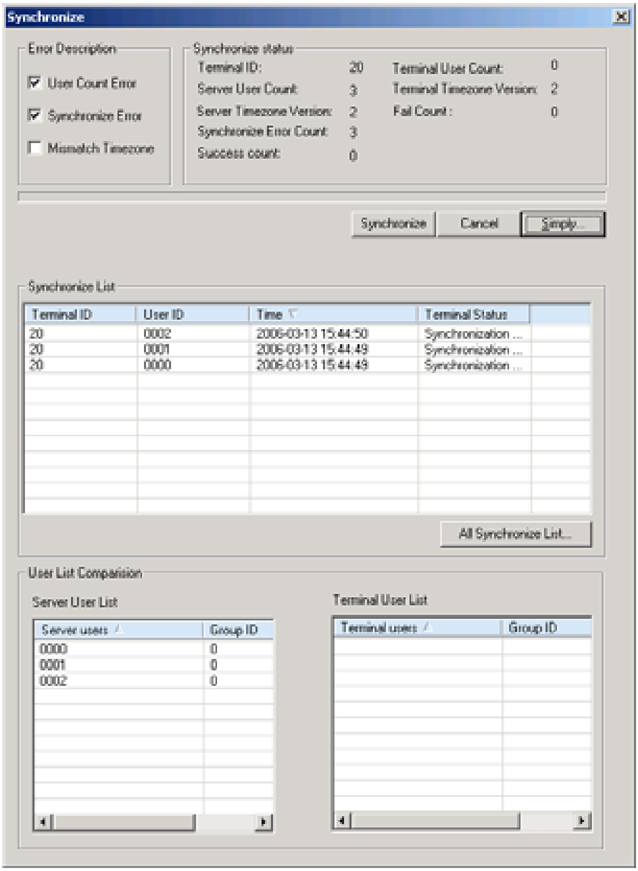
● **Synchronization**

If you click the **<Synchronize>** button, It corrects the synchronization errors between the server and the terminal.

● **Detail error information**

If you click the **<Detail…>** button, you can see the list of unsynchronized user information between the selected terminal and the server.

You can also compare the users registered on the server with those registered on the terminal.



Error Description

☑ User Count Error

☑ Synchronize Error

☐ Mismatch Timezone

Synchronize status

Terminal ID: 20

Server User Count: 3

Server Timezone Version: 2

Synchronize Error Count: 3

Success count: 0

Terminal User Count: 0

Terminal Timezone Version: 2

Fail Count : 0

Synchronize List

| Terminal ID | User ID | Time | Terminal Status |
|---|---|---|---|
| 20 | 0002 | 2006-03-13 15:44:50 | Synchronization ... |
| 20 | 0001 | 2006-03-13 15:44:49 | Synchronization ... |
| 20 | 0000 | 2006-03-13 15:44:49 | Synchronization ... |

User List Comparision

Server User List

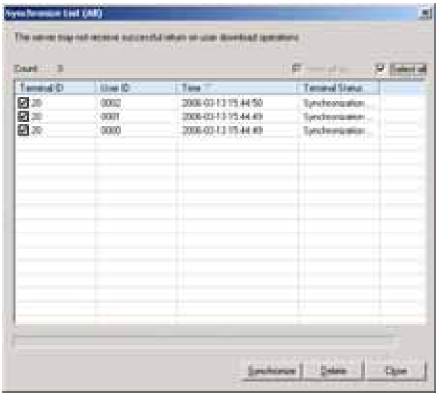
| Server users | Group ID |
|---|---|
| 0000 | 0 |
| 0001 | 0 |
| 0002 | 0 |

Terminal User List

| Terminal users | Group ID |
|---|---|

If you click the **<All Synchronize List>** button, the **Synchronize List (All)** window will appear for all users and terminals.

If you click the **<Synchronize>** button in the following window, the contents of the terminal will be modified in accordance with those of the server for the errors in the **Synchronize List**.



Synchronize List (All)

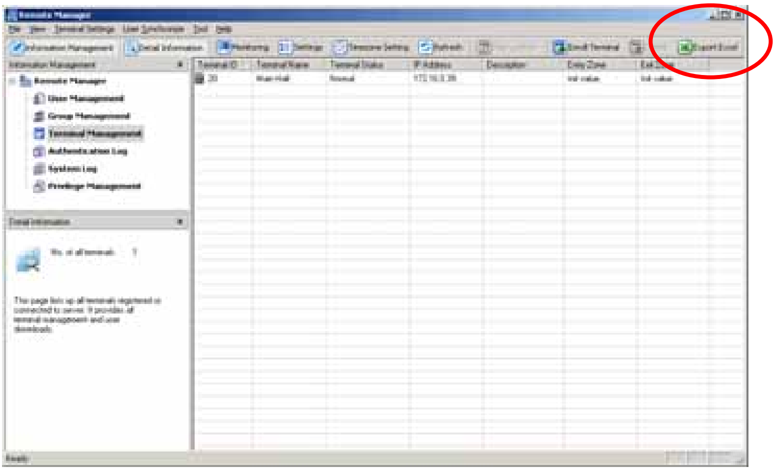
The server may not receive successful return on user download operations

Count: 3

| Terminal ID | User ID | Time | Terminal Status |
|---|---|---|---|
| ☑ 20 | 0002 | 2006-03-13 15:44:50 | Synchronization... |
| ☑ 20 | 0001 | 2006-03-13 15:44:49 | Synchronization... |
| ☑ 20 | 0000 | 2006-03-13 15:44:49 | Synchronization... |

## ● EXPORT EXCEL

The Terminal list on the screen can be exported and saved as Excel file by using “EXPORT EXCEL” Menu.



Remote Manager

| Terminal ID | Terminal Name | Terminal Status | IP Address | Description | Entry Zone | Exit Zone |
|---|---|---|---|---|---|---|
| 20 | Main Hall | Normal | 172.16.3.39 | | Init value | Init value |

No. of all terminals : 1

The page lists up all terminals registered or connected to server. It provides all terminal management and user downloads.

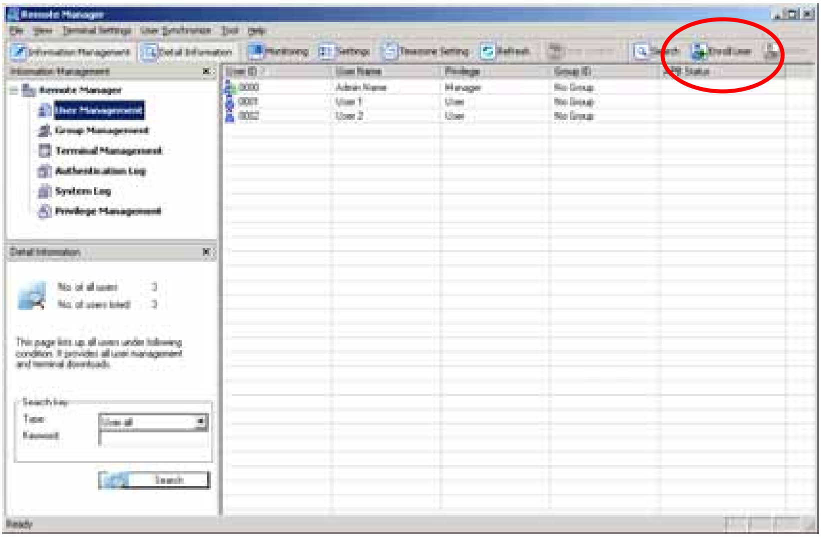
## 4.2 User Management

### ■ Enroll User

Enter and register basic information of a new user as follows:

(1) Select **User Management** in the **Information Management window**.

(2) Right-click **User Management** and select **Enroll User** from the submenu, or select **Enroll User** from the **Toolbar**.

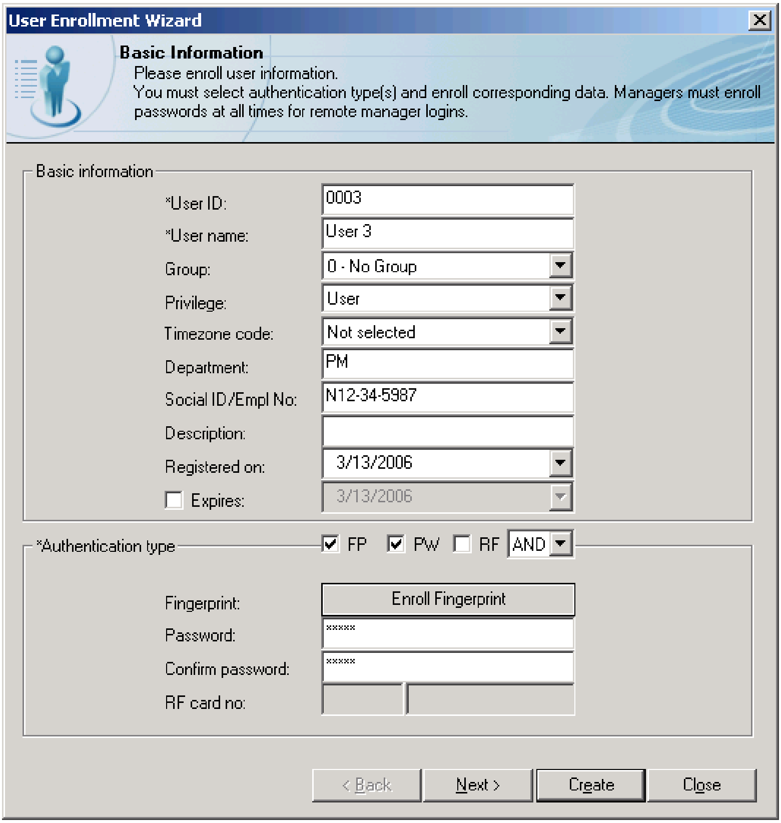


| User ID | User Name | Privilege | Group ID | APB Status |
|---|---|---|---|---|
| 0000 | Admin Name | Manager | No Group | |
| 0001 | User 1 | User | No Group | |
| 0002 | User 2 | User | No Group | |

No. of all users 3

No. of users listed 3

This page lists up all users under following condition. It provides all user management and terminal downloads.



User Enrollment Wizard

**Basic Information**

Please enroll user information.

You must select authentication type(s) and enroll corresponding data. Managers must enroll passwords at all times for remote manager logins.

Basic information

*User ID: 0003

*User name: User 3

Group: 0 - No Group

Privilege: User

Timezone code: Not selected

Department: PM

Social ID/Empl No: N12-34-5987

Description:

Registered on: 3/13/2006

□ Expires: 3/13/2006

*Authentication type ☑ FP ☑ PW □ RF AND

Fingerprint: Enroll Fingerprint

Password: *****

Confirm password: *****

RF card no:

When you finish the setup of basic information and authentication type, proceed with the buttons below.

**<Next>:** Proceed to the next step to add the user to or delete the user from terminals.

**<Create>:** Register another user.

**<Close>:** Cancel what you've done and exit the wizard window.

- **Basic Information**

• User ID:

Enter a user ID with the specified digit length.

• User name:

Enter a user name.

• Privilege:

Choose one of the followings: Manager, User, Guest and Power User. Manager can use the management programs, Remote Manager and Remote Monitor. User and Guest have no difference in privilege. But you can specify a temporary user as Guest for more efficient management. Power user can only use **Power User Privilege** functions.

(Please refer to **4.5 Program Options.)**

● Timezone code:

Select the timezone code to determine the allowed time for the user.

• Group:

Choose a group for a user.

• Social ID/Empl no:

Enter a Social ID or employee number of a user.

• Description:

Enter a brief user description.

• Registered on:

It indicates the date when a user has been registered. The date can be updated if the user is registered with download reservation.

- Expires:

  You can specify an expire date. After the specified date, user information is removed from the terminal and authentication for the user is not available.

- **Authentication type**

You can combine the following authentication types for your convenience: Fingerprint, Password and RF. For more information on how to use a terminal with different authentication types, refer to NAC-3000 Terminal User Manual.

- AND combination :

  Access authentication will complete only after all combined authentication types are validated.

- OR combination :

  Access authentication will complete after one of the authentication types in the combination is validated.

(1) Fingerprint

Fingerprints are pre-enrolled, and a user's fingerprint is compared to the pre-enrolled one when performing access authentication. (Refer to 3.2 Basic settings and running on how to enroll fingerprints.)

(2) Password

Authenticate with a pre-registered password (passwords can be 4~8 digits long.)

(3) RF card

Authenticate with an RF card. It is available only on terminals equipped with RF card module.

The RF card number consists of a site code and an RF card number. Therefore you must enter the site code and the RF card number separately.

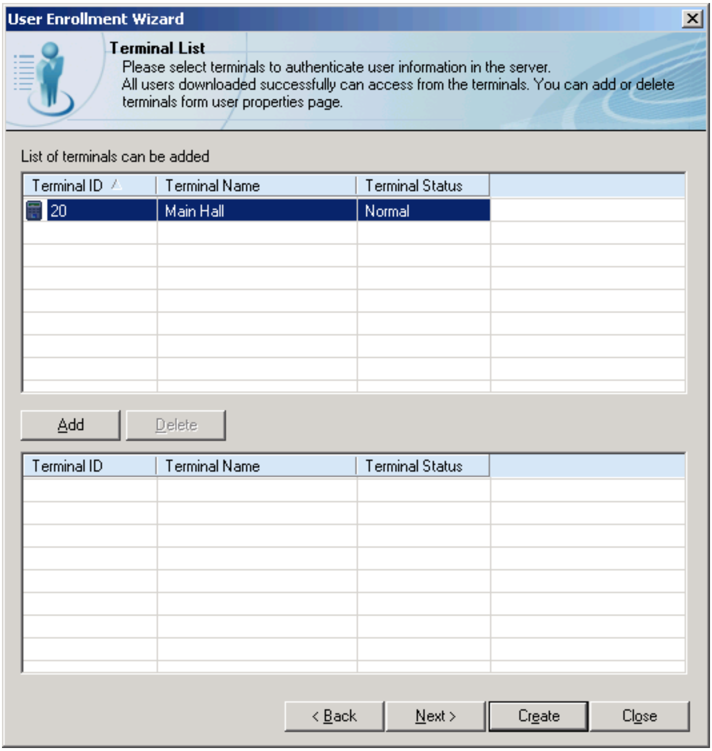
⚠ The users who required to authenticate at the Server side, cannot use RF Card authentication without putting user ID first. (However, the users who registered and authenticate at the Terminal side, RF Card authentication can be used.)
⚠ If you want RF Card authentication to be able to use for Server authentication users, please ask to NITGEN Co., Ltd.

When basic information and authentication type are selected, please refer to the following explanations on each button to proceed.

**<Next>:** to register users to a relevant terminal as server-authenticated user or delete the user.

**<Create>:** to complete the registration and to start the registration process for a new user.

**<Close>:** to cancel what have been typed in and to close the wizard window.


User Enrollment Wizard

**Terminal List**

Please select terminals to authenticate user information in the server.
All users downloaded successfully can access from the terminals. You can add or delete terminals form user properties page.

List of terminals can be added

| Terminal ID | Terminal Name | Terminal Status |
|---|---|---|
| 20 | Main Hall | Normal |

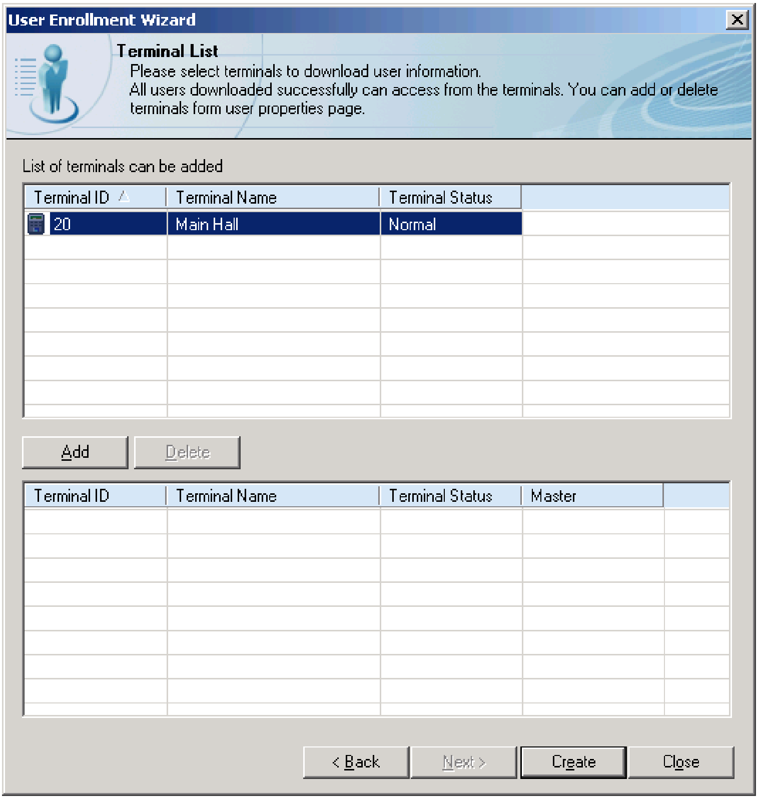
| Terminal ID | Terminal Name | Terminal Status |
|---|---|---|

Select the desired terminal at the top of the screen and then click on **<Add>** button to add a new terminal at the bottom part. When selecting a terminal at the bottom part of the screen and clicking on a **<Delete>** button, the relevant terminal will be deleted from the list.

**<Next>:** to register users to a relevant terminal as terminal-authenticated user or delete the user.

**<Create>:** to complete the registration and to start the registration process for a new user.

**<Close>:** to cancel what have been typed in and to close the wizard window.



User Enrollment Wizard

**Terminal List**

Please select terminals to download user information.
All users downloaded successfully can access from the terminals. You can add or delete terminals form user properties page.

List of terminals can be added

| Terminal ID | Terminal Name | Terminal Status |
|---|---|---|
| 20 | Main Hall | Normal |

| Terminal ID | Terminal Name | Terminal Status | Master |
|---|---|---|---|

Select the desired terminal at the top of the screen and then click on **<Add>** button to add a new terminal at the bottom part. When selecting a terminal at the bottom part of the screen and clicking on a **<Delete>** button, the relevant terminal will be deleted from the list. A master can select the type of user right for terminals on the list.

**<Create>:** to complete the registration and to start the registration process for a new user.

**<Close>:** to cancel the procedures.

## ■ Delete User

You can delete users registered in the server. If the terminal is connected to the network, user information in the terminal will also be deleted. If you want to delete users from the terminal, not from the server, use User List in the Terminal Properties window.

You can delete a user as follows:

(1) Select User Management in the **Information Management window**.

(2) Select the user you want to delete in the **List window**, and click the **Delete** button from the toolbar. Alternatively, you can use the **<Delete>** key on the keyboard or click the right mouse button to select **Delete** from the submenu.

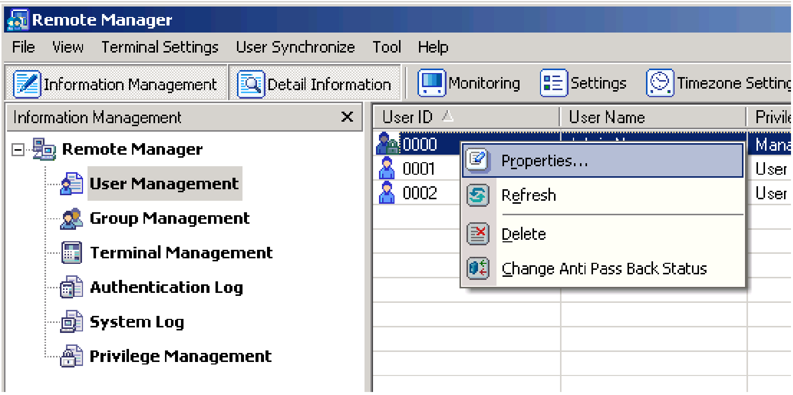
You can choose multiple users in the **List window** using the **<Shift>** or **<Ctrl>** key to delete them at once.

## ■ Check/Change User Properties

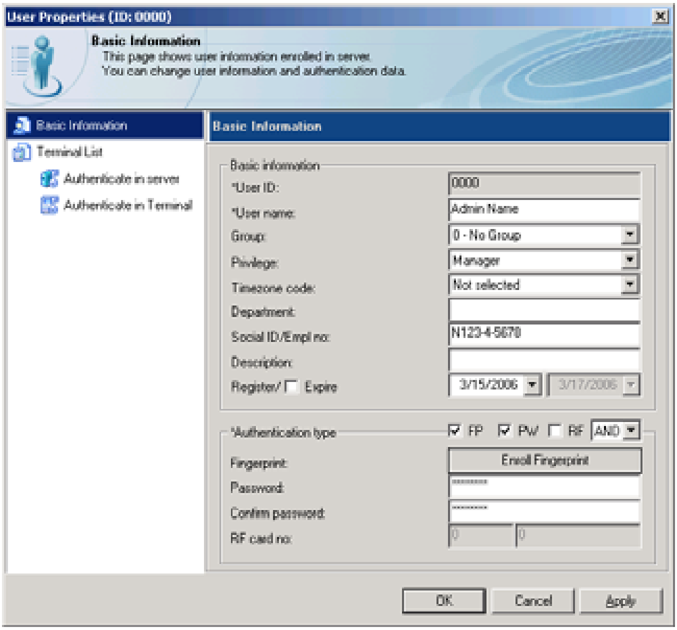
You can check or change basic information and available terminals for a user.

(1) Select **User Management** in the **Information Management window**.

(2) Double-click a user in the **List window**, or right-click a user and choose **Properties** from the submenu.



(3) In the below **User Properties** window, you can change basic user information. To change available terminals for a user, select **Terminal List** from the menu on the left.



Basic information

| | |
|---|---|
| *User ID: | 0000 |
| *User name: | Admin Name |
| Group: | 0 - No Group |
| Privilege: | Manager |
| Timezone code: | Not selected |
| Department: | |
| Social ID/Empl no: | N123-4-5678 |
| Description: | |
| Register/ □ Expire | 3/15/2006 3/17/2006 |

*Authentication type ☑ FP ☑ PW □ RF AND

| | |
|---|---|
| Fingerprint: | Enroll Fingerprint |
| Password: | ******** |
| Confirm password: | ******** |
| RF card no: | 0 0 |

The rest of the procedure is the same as that of user registration.

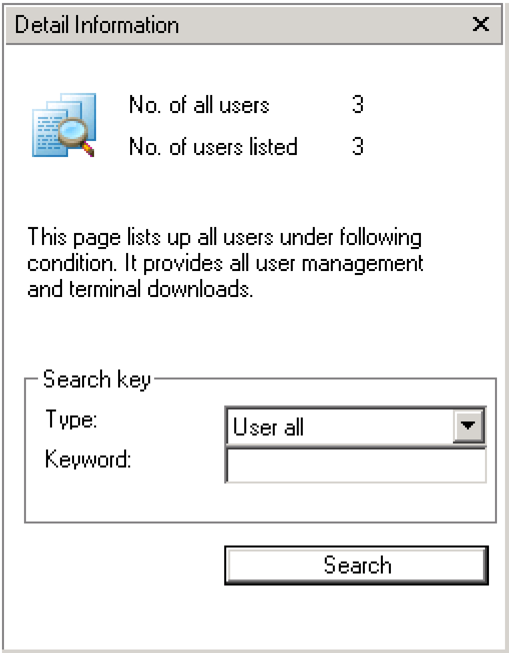
## ■ User Search

If there are many users in the database, you can easily search users with search conditions.

You can search users in the following way, and the search result will be displayed in the **List window**.

(1) Select **User Management** in the **Information Management window**.

(2) If the **Detail Information** button is selected in the toolbar, you can perform search in the **Detail Information** window as below. Or, click the search button in the toolbar to open the **User Search** window.



Detail Information

No. of all users 3

No. of users listed 3

This page lists up all users under following condition. It provides all user management and terminal downloads.

Search key

Type: User all

Keyword:

- Search type

You can choose such condition as All users, user ID, user name, group ID, terminal ID or Social ID/Empl no.

- Keyword

Depending on the search condition you choose, you can enter an ID or name.

- Export Excel

The user information can be saved as Excel file.

To choose “Export Excel” on the Menu bar.

## 4.3 Group Management

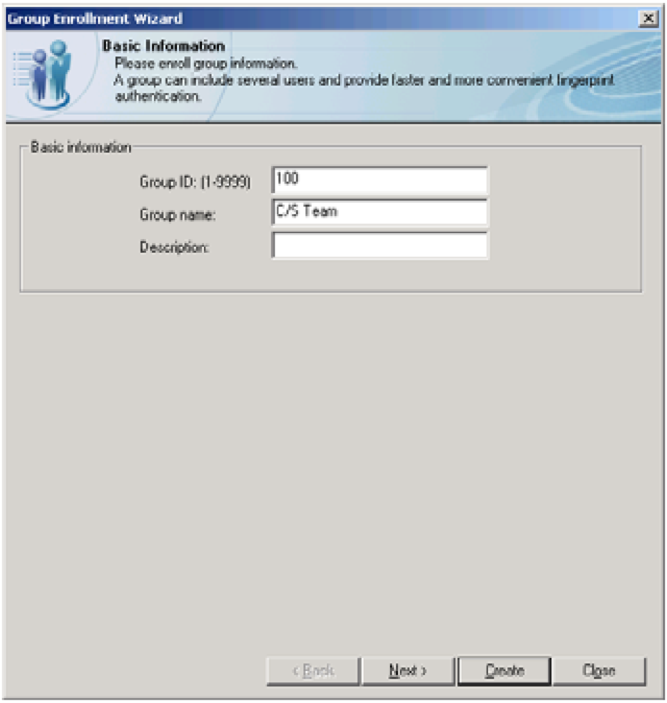
You can register or delete groups, and add or delete users in a group.

### ■ Enroll Group

(1) Select **Group Management** in the **Information Management window**.

(2) Click the right mouse button to select **Enroll Group** from the submenu or click the **Enroll Group** button from the toolbar.

(3) When the following window appears, enter group ID, group name, and description, and click **<Next>** to add or delete users in the group.



Group Enrollment Wizard

Basic Information

Please enroll group information.

A group can include several users and provide faster and more convenient fingerprint authentication.

Basic information

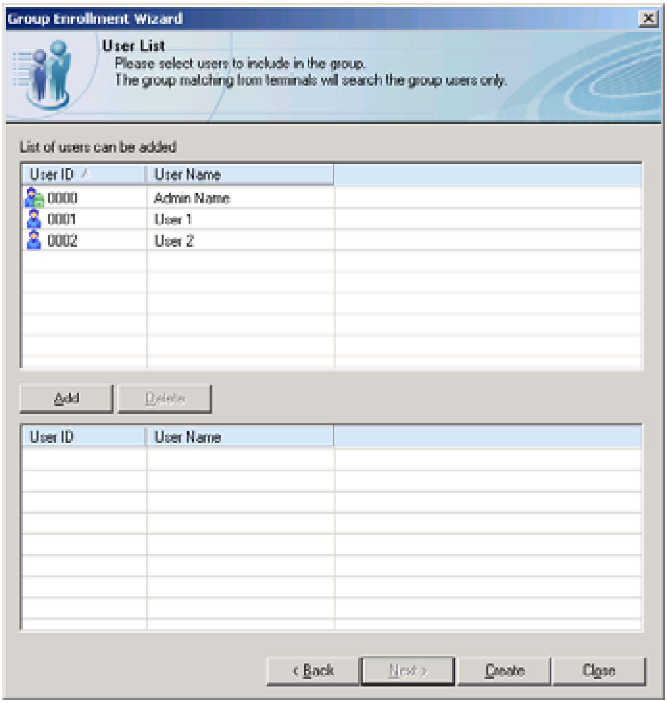
Group ID: (1-9999) 100

Group name: C/S Team

Description:

**<Create>:** Complete the registration and add another group.

**<Close>:** Cancel what you've done so far.



Group Enrollment Wizard

User List

Please select users to include in the group.
The group matching from terminals will search the group users only.

List of users can be added

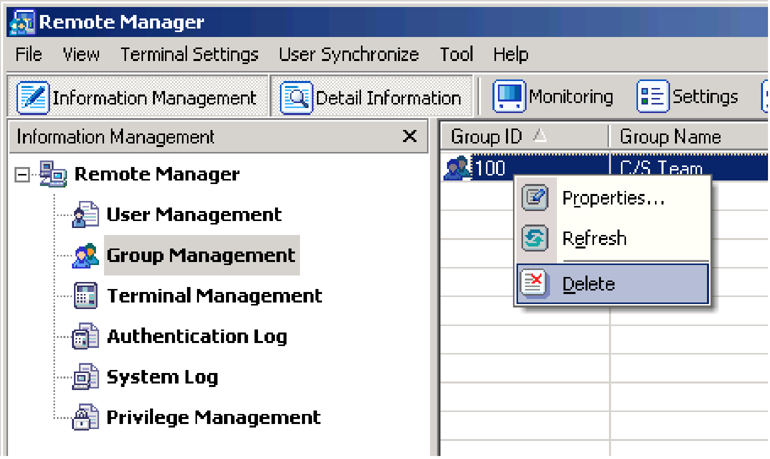
| User ID | User Name |
|---|---|
| 0000 | Admin Name |
| 0001 | User 1 |
| 0002 | User 2 |

## ■ Delete Group

You can delete a group as follows:

(1) Select **Group Management** in the **Information Management window**.

(2) Select the group you want to delete in the **List window**, and click the **Delete** button from the toolbar. Alternatively, you can use the **<Delete>** key on the keyboard or click the right mouse button to select **Delete** from the submenu.



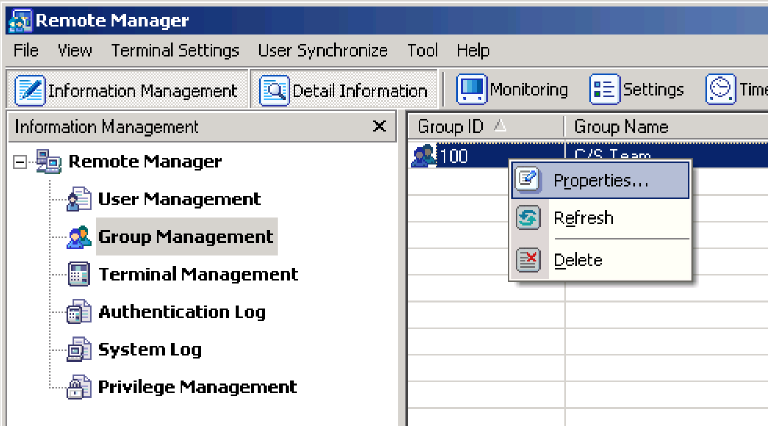
You can choose multiple groups in the **List window** using the **<Shift>** or **<Ctrl>** key to delete them at once.

## ■ Check/Change Group Properties

You can check or change basic information and user list for a group.

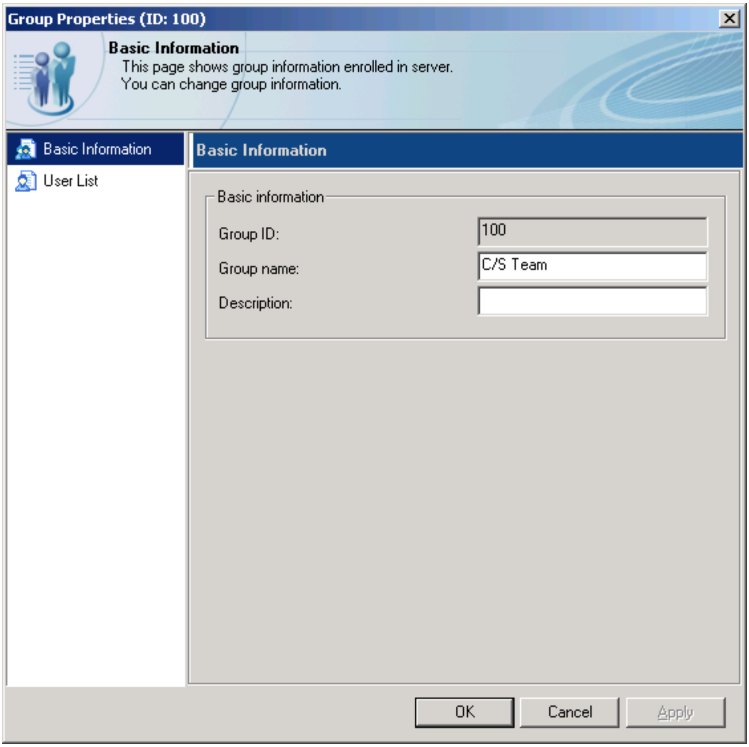
(1) Select **Group Management** in the **Information Management window**.

(2) Double-click a group in the **List window**, or right-click a group to select **Properties** from the submenu.



(3) In the following **Group Properties** window, you can change basic information. To add or delete users in the group, select **User List** from the menu on the left.

The rest of the procedure is the same as that of group registration.



Group Properties (ID: 100)

Basic Information

This page shows group information enrolled in server.
You can change group information.

Group ID: 100

Group name: C/S Team

Description:

- Export Excel

The user information can be saved as Excel file.

To choose “Export Excel” on the Menu bar.

## 4.4 Log Management

### ■ Authentication log management

You can check and manage terminal access authentication log.

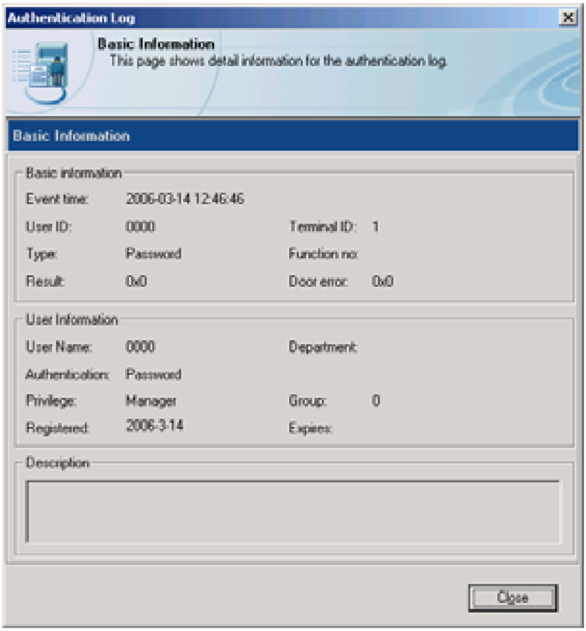
- **Log Properties**

You can check authentication log in the following way, and the search result will be displayed in the **List window**.

(1) Select **Authentication Log** in the **Information Management window.**

(2) You can check authentication log information in the **List window**.

(3) To see detailed information, double-click a log or click the right mouse button to select **Properties** from the submenu.



Basic Information
This page shows detail information for the authentication log.

Basic Information

Basic information

| | | | |
|---|---|---|---|
| Event time: | 2006-03-14 12:46:46 | | |
| User ID: | 0000 | Terminal ID: | 1 |
| Type: | Password | Function no: | |
| Result: | 0x0 | Door error: | 0x0 |

User Information

| | | | |
|---|---|---|---|
| User Name: | 0000 | Department: | |
| Authentication: | Password | | |
| Privilege: | Manager | Group: | 0 |
| Registered: | 2006-3-14 | Expires: | |

Description

- **Export Excel**

You can save the log information as an Excel file.

(1) Select **Authentication Log** in the **Information Management window**.

(2) Click the right mouse button to select **Export Excel** from the submenu, or select **Export Excel** from the toolbar.

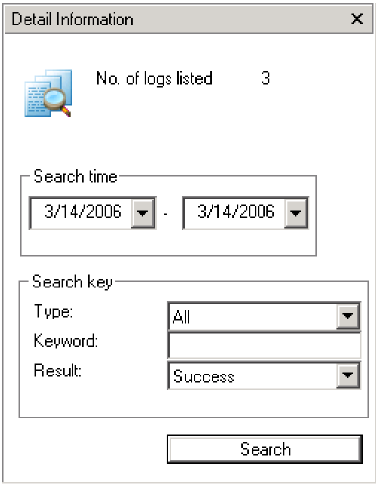
(3) Specify the location and file name, and click **<Save>.**

- **Authentication Log Search**

If the log information is very large, you can search necessary information as follows:

(1) Select **Authentication Log** in the **Information Management window**.

(2) If the **Detail Information** button is selected in the toolbar, you can perform search in the **Detail Information** window as below. Or, click the search button in the toolbar to open the **Authentication Log Search** window.



Detail Information

No. of logs listed 3

Search time

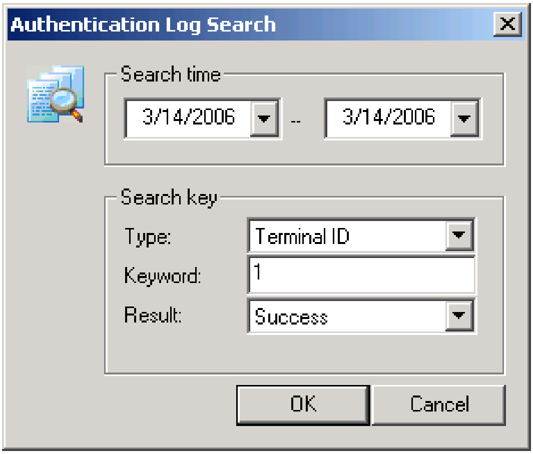
3/14/2006 - 3/14/2006

Search key

Type: All

Keyword:

Result: Success



3/14/2006 -- 3/14/2006

Type: Terminal ID

Keyword: 1

Result: Success

## ■ System Log Management

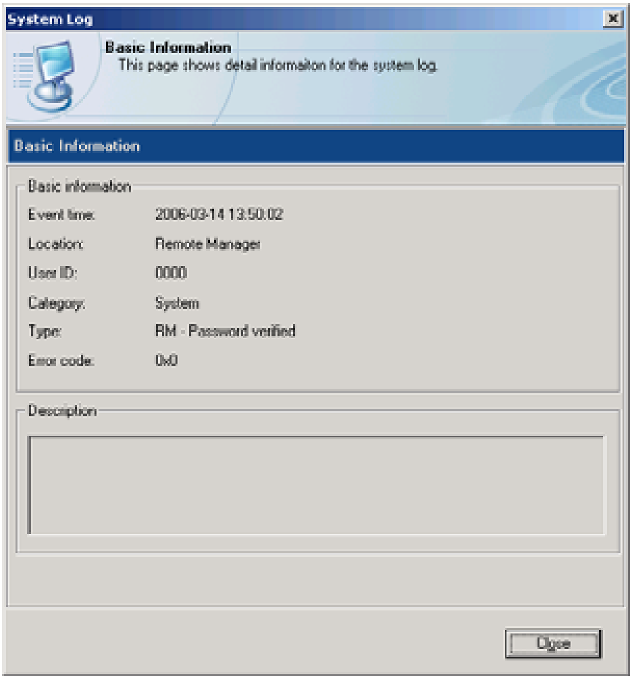
You can see system log information on program executions.

### ● System Log Information

(1) Select **System Log** in the **Information Management window**.

(2) You can check system log information in the **List window.**

(3) To see detailed information, double-click a log or click the right mouse button to select **Properties** from the submenu.



Basic Information

This page shows detail informaiton for the system log.

Basic information

Event time: 2006-03-14 13:50:02

Location: Remote Manager

User ID: 0000

Category: System

Type: RM - Password verified

Error code: 0x0

Description

**Location** is the terminal ID where the event took place. If this value is **Remote Manager**, it means that the event is related with Remote Manager.

- **Export Excel**

You can save log information as an Excel file.

(1) Select **System Log** in the **Information Management window**.

(2) Click the right mouse button to select **Export Excel** from the submenu, or select **Export Excel** from the toolbar.

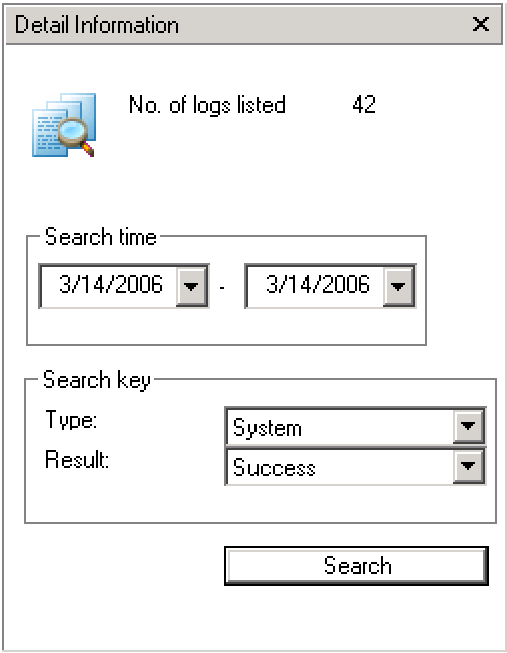
(3) Specify the folder and name for the file, and click **<Save>**.

- **System Log Search**

If the log information is very large, you can search necessary information in the following way, and the search result will be displayed in the **List window**.

(1) Select **System Log** in the **Information Management window**.

(2) If the **Detail Information** button is selected in the toolbar, you can perform search in the **Detail Information** window as below. Or, click the Search button in the toolbar to open the **System Log Search** window.



Detail Information

No. of logs listed 42

Search time

3/14/2006 - 3/14/2006

Search key

Type: System

Result: Success

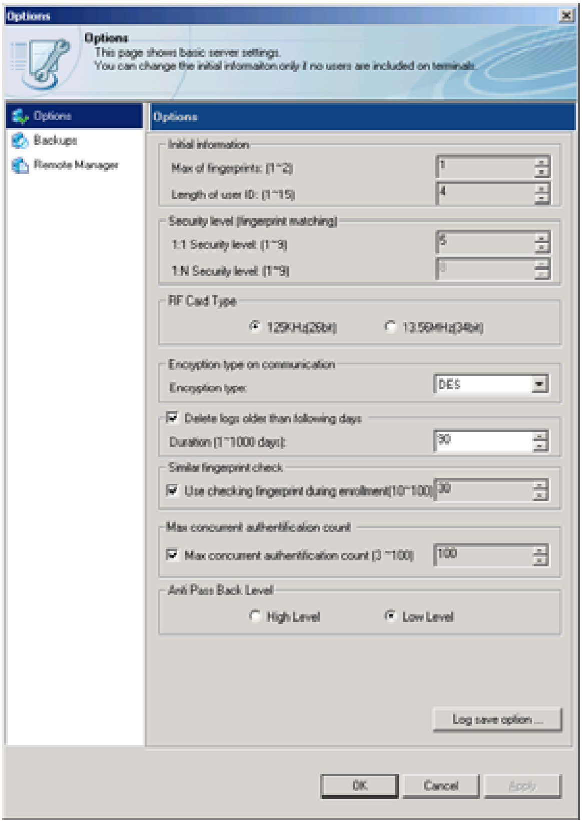
## 4.5 Program Options

You can check or change the initial program settings.

Select **Tool > Settings** from the menu bar**,** or click the **Settings** button from the toolbar to open the **Options** window.

### ■ Basic Server Settings

In the initial **Options** window, you can see the basic server settings. For more information on the settings, refer to **3.2 Basic settings and running**.



**Options**
This page shows basic server settings.
You can change the initial informaiton only if no users are included on terminals.

Initial information
Max of fingerprints: (1~2) 1
Length of user ID: (1~15) 4

Security level (fingerprint matching)
1:1 Security level: (1~9) 5
1:N Security level: (1~9) [illegible]

RF Card Type
● 125KHz(26bit) ○ 13.56MHz(34bit)

Encryption type on communication
Encryption type: DES

☑ Delete logs older than following days
Duration (1~1000 days): 30

Similar fingerprint check
☑ Use checking fingerprint during enrollment(10~100) 30

Max concurrent authentification count
☑ Max concurrent authentification count (3 ~100) 100

Anti Pass Back Level
○ High Level ● Low Level

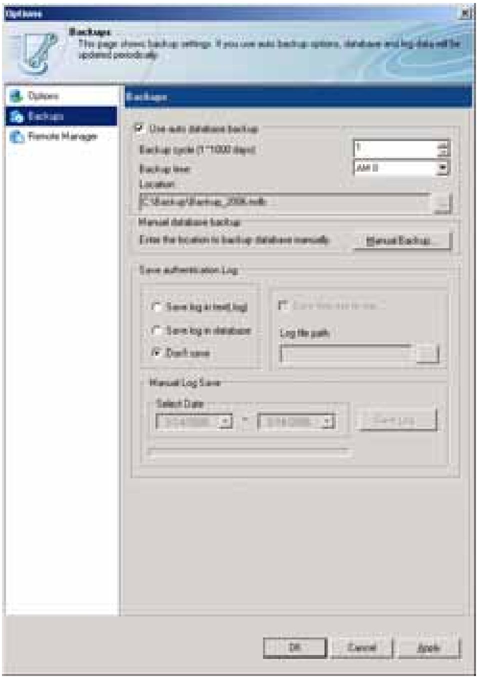
⚠ To increase the value of **max of fingerprints** or **length of user ID**, delete all terminal users and set the value again. And then re-register users by terminal.

⚠ To decrease the value of **max of fingerprints** or **length of user ID**, you must delete all users registered in the server as well as in the terminal.

■ **Server Backup Settings**

Select **Backups** from the menu on the left of the **Options** window.

For more information on the settings, refer to **3.2 Basic settings and running**.



Options

Backups

This page shows backup settings. If you use auto backup options, database and log data will be updated periodically.

Backups

☑ Use auto database backup

Backup cycle (1~1000 days): 1

Backup time: AM 0

Location: C:\Backup\Backup_2006.mdb

Manual database backup

Enter the location to backup database manually

Save authentication Log

○ Save log at text(.log)

○ Save log in database

● Don't save

□ [illegible]

Log file path

Manual Log Save

Select Date

- Manual Saving of Log Files

This will be activated when the above ‘log(.log) file save’ is selected.

To save text log, select the date and then click <**Save Log..**> button to select the name of log that will be saved. Click OK when done.

When ‘Save files day-by-day’check box is selected, text log will be saved on a day-by-day basis.

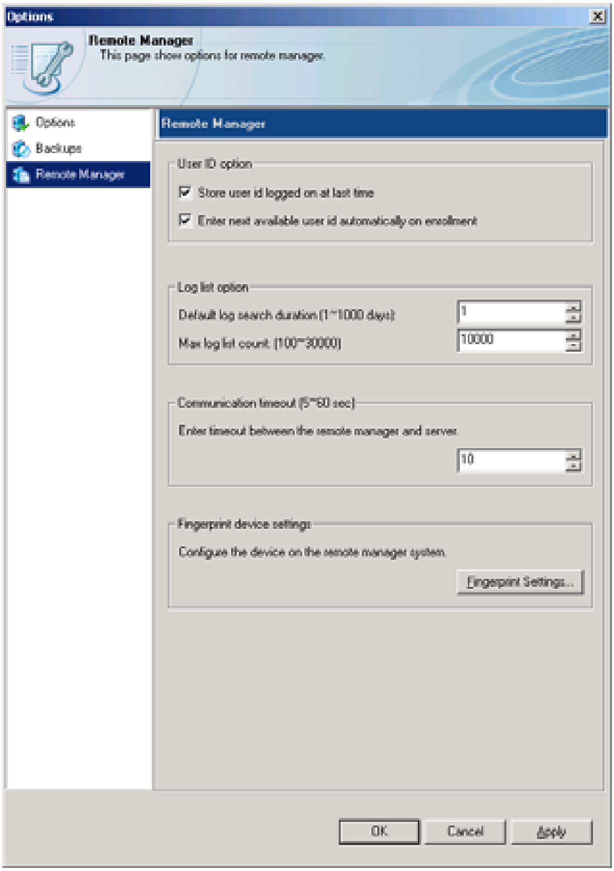
However, this function will be available only when the server and remote admin program are located in the same position.

Ex) If the text log name is set as ‘textlog.log’ and the log date range is from 12/9/2005 to 13/9/2005.

1. When ‘Save files day-by-day’is not selected, ‘textlog.log’ will save all the details of the log.
2. When ‘Save files day-by-day’ is selected, ‘textlog_20050912.log’, ‘textlog_20050913.log’and similar types will be used.

## ■ Remote Manager Settings

Select **Remote Manager** from the menu on the left of the **Options** window.



Remote Manager

This page show options for remote manager.

User ID option

☑ Store user id logged on at last time

☑ Enter next available user id automatically on enrollment

Log list option

Default log search duration (1~1000 days): 1

Max log list count (100~30000): 10000

Communication timeout (5~60 sec)

Enter timeout between the remote manager and server. 10

Fingerprint device settings

Configure the device on the remote manager system.

### • User ID option

(1) Store user id logged on at last time

This feature automatically enters the manager's login ID at program login.

(2) Enter next available user id automatically on enrollment

When you register multiple users one by one, this feature automatically generates the next ID incremented by 1.

- **Log list option**

(1) Default log search duration (1~1000 day)

You can specify the basic search period. If you do not change the value, the **List window** will show logs with the default.

(2) Max log list count (100 ~ 30000)

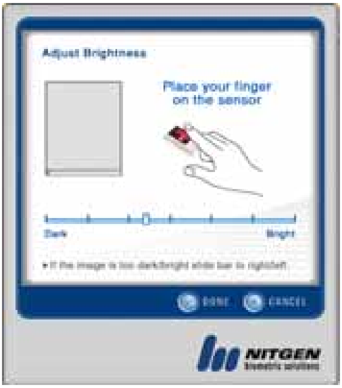
You can specify the number of logs to be displayed in the **List window** between 100 and 30,000.

- **Communication timeout (5~60sec)**

You can specify a value between 5 and 60. If there is no response within the specified time limit, it will be assumed that there is no network connection. If the network environment is not stable, increase the value gradually.

- **Fingerprint device settings**

By properly adjusting the brightness of the fingerprint device used by the remote management program, you can get clearer images.

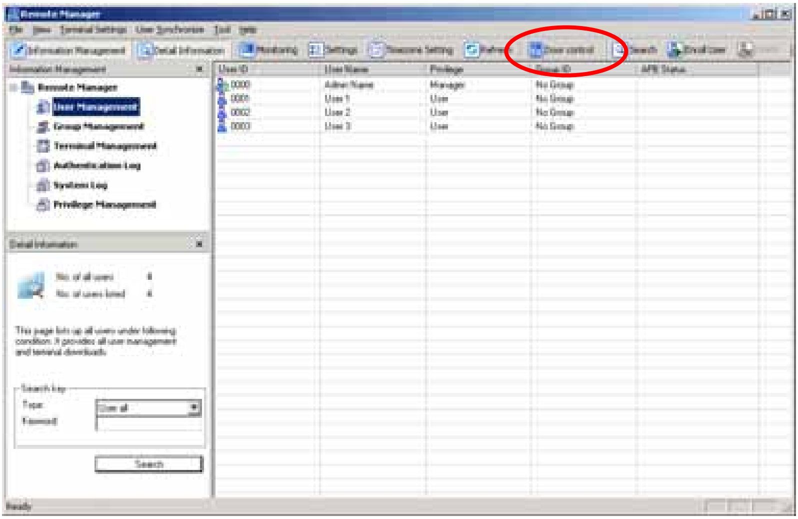


• If the image is too dark/bright slide bar to right/left

- **Enable Control Gate Function**

An administrator can force open or close a door associated with a specific terminal through remote controlling. If this option is selected, **<Door control>** menu in a remote admin tool bar is activated.

Please refer to toolbar in part **3.3 About Menu**.



| User ID | User Name | Privilege | Group ID | APB Status |
|---|---|---|---|---|
| 0000 | Admin Name | Manager | No Group | |
| 0001 | User 1 | User | No Group | |
| 0002 | User 2 | User | No Group | |
| 0003 | User 3 | User | No Group | |

No. of all users 4

No. of users listed 4

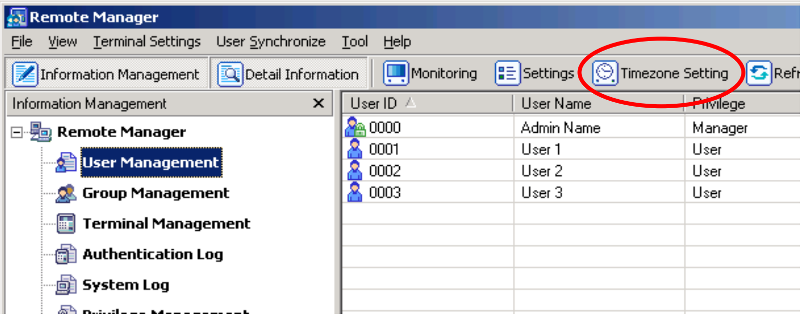
This page lists up all users under following condition. It provides all user management and terminal downloads.

Type: User all

## 4.6 Timezone Setting

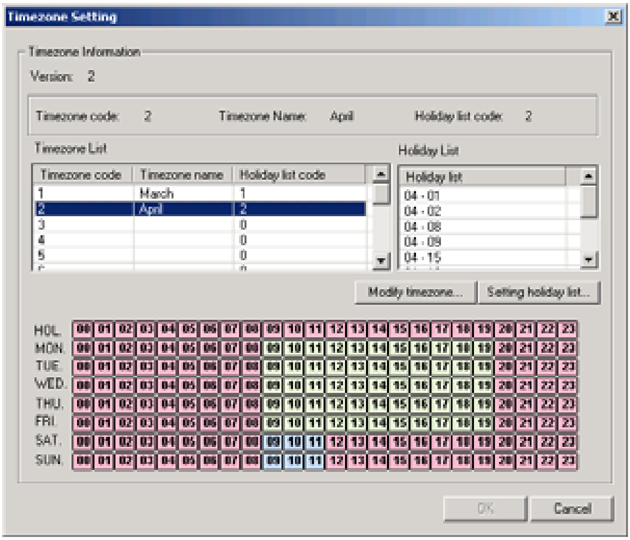
You can use this window to set up the allowed or restricted time for the terminal or the user.

Select **Timezone Setting** from the toolbar.



| User ID | User Name | Privilege |
|---|---|---|
| 0000 | Admin Name | Manager |
| 0001 | User 1 | User |
| 0002 | User 2 | User |
| 0003 | User 3 | User |

The following **Timezone Setting** window will appear.



Version: 2

Timezone code: 2 Timezone Name: April Holiday list code: 2

| Timezone code | Timezone name | Holiday list code |
|---|---|---|
| 1 | March | 1 |
| 2 | April | 2 |
| 3 | | 0 |
| 4 | | 0 |
| 5 | | 0 |

| Holiday list |
|---|
| 04 - 01 |
| 04 - 02 |
| 04 - 08 |
| 04 - 09 |
| 04 - 15 |

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| HOL. | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| MON. | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| TUE. | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| WED. | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| THU. | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| FRI. | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| SAT. | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| SUN. | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |

As shown above, the timezone set has 16 timezones and 16 holiday lists. The timezone has a timetable with days of the week such as holiday, Monday, Tuesday, etc. And the holiday list allows you to register 30 dates.

You can link each timezone to one of the 16 holiday lists.

In the above figure, for example, timezone #1 is for common employees and uses holiday list #1 among the 16 holiday lists.

As any access is denied for the entire 24 hours for holiday list, terminals set for common users cannot have an access on a specific date under holiday list.

For Saturdays and Sundays, doors are set open from 9:00 AM to 12:00 PM, and users can have an access without authentication. For weekdays, users can have an access between 9:00 AM to 8:00 PM depending on the result of authentication. Access is denied for other times.

You can set timezone by individual user or by terminal, and you can also set it by combining them. To restrict access time only by user, set the timezone code for the terminal as **Not selected**.

To restrict access time only by terminal, set the timezone code for all users as **Not selected**.

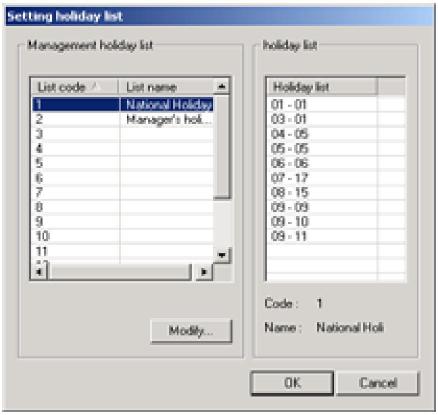
When you combine two methods, the priority is as below.

⚠ **Priority affected by the timezone code**

- Time for door opening set at terminal > Holidays of the timezone set for the terminal > common days of the week set for the terminal > holidays set for the user > common days of the week set for the user
- Even when a user uses a timezone code, entrance will be restricted for the user if the time is not allowed on the terminal to which the user belongs.

## ● Modify holiday lists

As default, there are 16 holiday lists that remain unconfigured. There is no registration procedure.
To specify a certain date as a holiday, click the **<Setting holiday list>** button in the **Timezone Setting** window.
This window shows all holiday lists.



Setting holiday list

Management holiday list

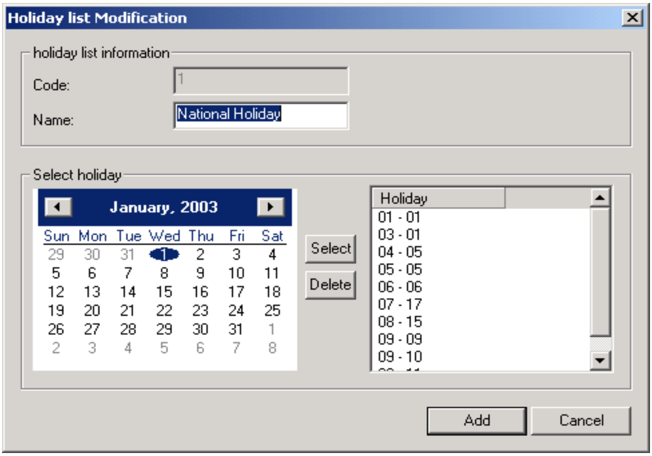
| List code | List name |
|---|---|
| 1 | National Holiday |
| 2 | Manager's hol... |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| 7 | |
| 8 | |
| 9 | |
| 10 | |
| 11 | |

holiday list

| Holiday list |
|---|
| 01 - 01 |
| 03 - 01 |
| 04 - 05 |
| 05 - 05 |
| 06 - 06 |
| 07 - 17 |
| 08 - 15 |
| 09 - 09 |
| 09 - 10 |
| 09 - 11 |

Code : 1
Name : National Holi

Select the holiday code you want to edit from **Management holiday list**, and click the **<Modify>** button.



Holiday list Modification

holiday list information
Code: 1
Name: National Holiday

Select holiday

January, 2003

| Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|---|---|---|---|---|---|---|
| 29 | 30 | 31 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 26 | 27 | 28 | 29 | 30 | 31 | 1 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |

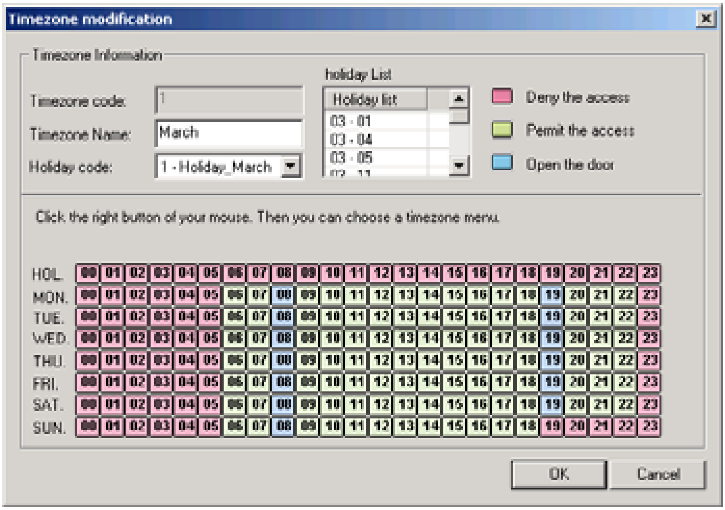
| Holiday |
|---|
| 01 - 01 |
| 03 - 01 |
| 04 - 05 |
| 05 - 05 |
| 06 - 06 |
| 07 - 17 |
| 08 - 15 |
| 09 - 09 |
| 09 - 10 |

Enter the name of the holiday list, and select a date from the **Select holiday** section. Click the **<Select>** button to add the date to the holiday list. Select up to 30 dates repeatedly and click the **<Add>** button to make one holiday list. To delete a date from the holiday list, select the date and click the **<Delete>** button.

● **Timezone modification**

By default, there are 16 holiday lists that remain unconfigured. In other words, entrance is allowed at any time. There is no registration procedure.

Click the **<Modify timezone>** button in the **Timezone Setting** window.



Timezone modification

Timezone Information

Timezone code: 1

Timezone Name: March

Holiday code: 1 - Holiday_March

holiday List

| Holiday list |
|---|
| 03 - 01 |
| 03 - 04 |
| 03 - 05 |

🟥 Deny the access

🟩 Permit the access

🟦 Open the door

Click the right button of your mouse. Then you can choose a timezone menu.

| | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| HOL. | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 |
| MON. | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟦 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟦 | 🟩 | 🟩 | 🟩 | 🟥 |
| TUE. | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟦 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟦 | 🟩 | 🟩 | 🟩 | 🟥 |
| WED. | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟦 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟦 | 🟩 | 🟩 | 🟩 | 🟥 |
| THU. | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟦 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟦 | 🟩 | 🟩 | 🟩 | 🟥 |
| FRI. | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟦 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟦 | 🟩 | 🟩 | 🟩 | 🟥 |
| SAT. | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟦 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟦 | 🟩 | 🟩 | 🟩 | 🟥 |
| SUN. | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟦 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 |

Enter the name of the timezone, select the holiday code you want, and then select the allowed time for each day of the week. To set time for days of the week, click the mouse on a restricted time cell and drag it to other desired time cells. Then their status will change to allowed time. If you click the mouse on an allowed time cell and drag it to other cells, their status will change to restricted time.

If you click the right button of your mouse, you can choose a timezone menu.
If you click the **<OK>** button, a timezone will be created.
Once you create a holiday list and a timezone, you must click the **<OK>** button in the **Timezone Setting** window.
The new timezone information will be applied to all connected terminals in normal status.

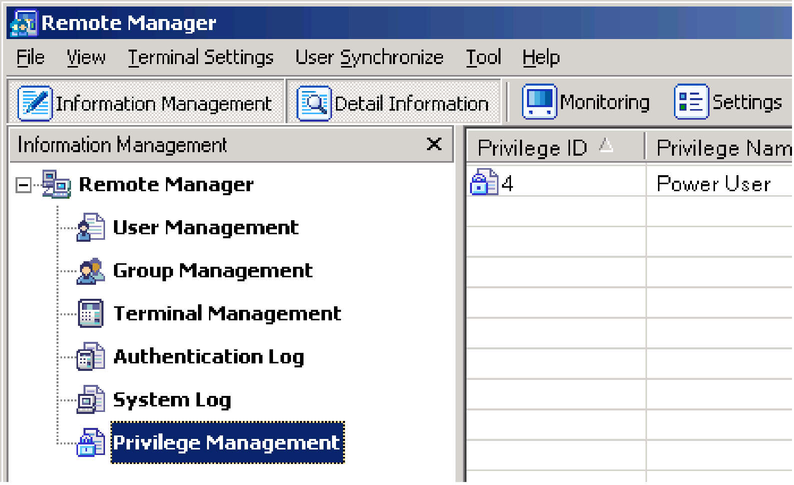
Existing NAC-3000 terminals with a designated timezone may show a message for synchronization.

This is due to errors in the version of timezone. Therefore, you have to run of **<synchronization>.**

NAC-3000 teminal don't have the time that a entry is always opened. (NAC-3000 will be upgraded in later versions.)

## 4.7 Privilege management

On top of the functions for basic administrator, users can create privilege management functions for selected functions, users and terminals.



| Privilege ID | Privilege Nam |
|---|---|
| 4 | Power User |

The menu can be controlled only by administrators, which include remote control programming and privilege for specific users and terminals.

Users with designated IDs with privilege can exercise the rights associated with the ID.

## ■ To register new privileges

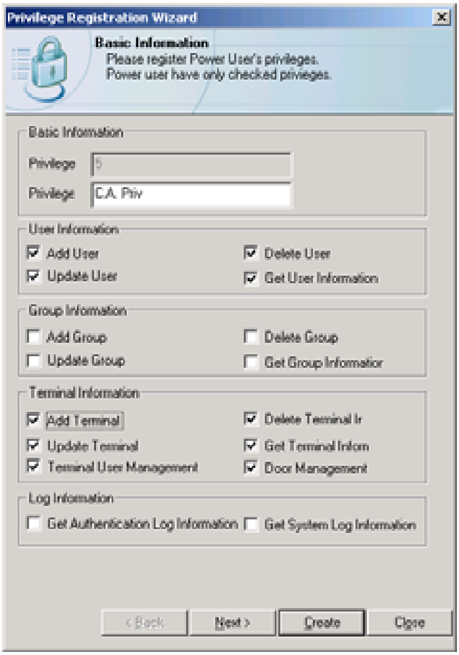
New privileges can be created in order to allocate specific privileges to users other than administrator.

It applies to specific functionality, users subject to management for specific privileges and terminals.

(1) Please select "privilege management" in the information management window.

(2) By doing a right mouse click, users can select "privilege registration." Or please click a button for "privilege registration" in the tool bar.

(3) If the following window pops up, please enter relevant ID and the name of privilege and check the functions. By clicking a <Next (N)> button, users can add or delete terminals subject to management with the allocated privilege.



Privilege Registration Wizard

Basic Information
Please register Power User's privileges.
Power user have only checked priviges.

Basic Information
Privilege: 5
Privilege: C.A. Priv

User Information
☑ Add User ☑ Delete User
☑ Update User ☑ Get User Information

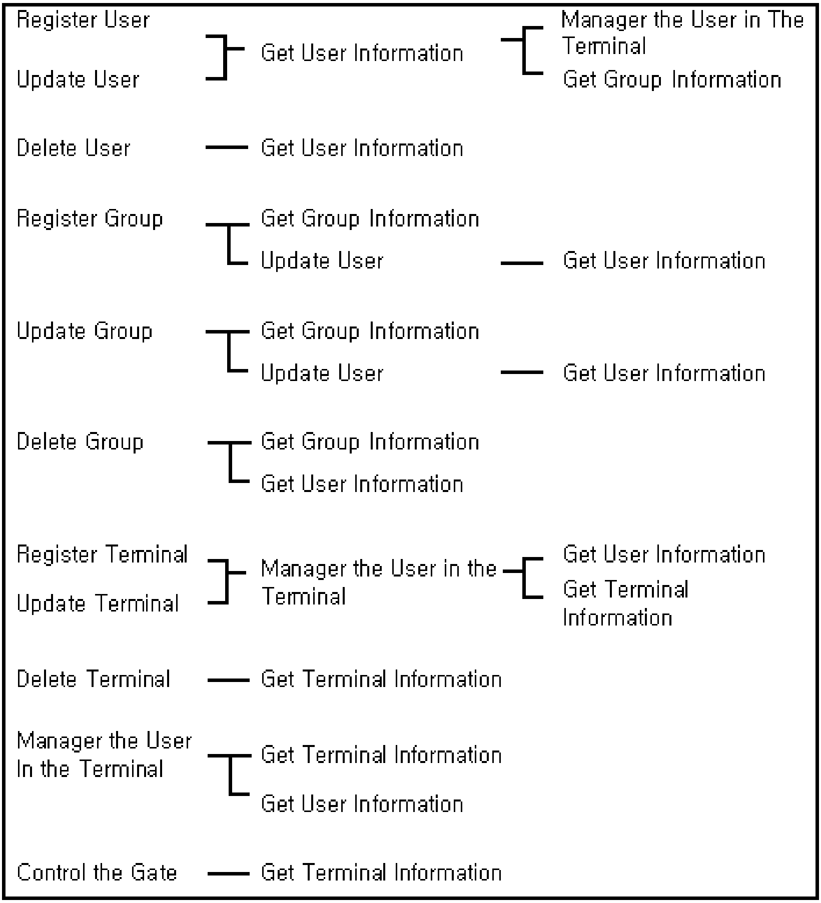
Group Information
☐ Add Group ☐ Delete Group
☐ Update Group ☐ Get Group Informatior

Terminal Information
☑ Add Terminal ☑ Delete Terminal Ir
☑ Update Terminal ☑ Get Terminal Infom
☑ Terminal User Management ☑ Door Management

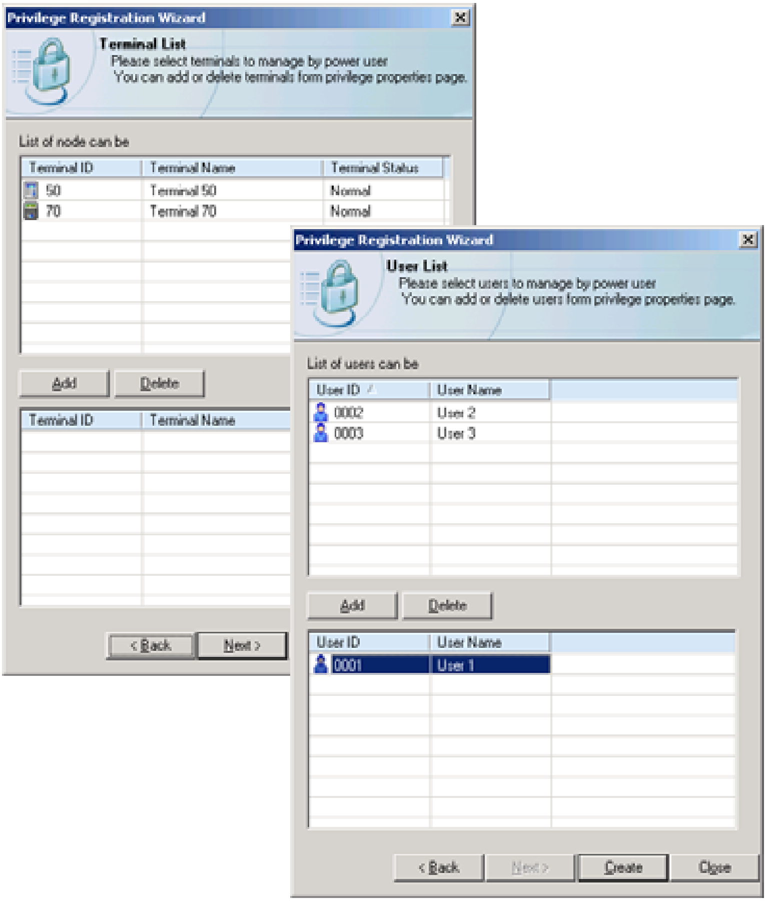
Log Information
☐ Get Authentication Log Information ☐ Get System Log Information

The following shows hierarchy of each menu. When selecting menu on the left side, functions on the right side will automatically be selected.

(When the higher level of menu is selected, you cannot de-activate the subordinate functions.)



(4) After selecting terminals subject to management from a list of terminals, please click a <Next(N)> button in order to add or delete users who have an appropriate privilege.



Privilege Registration Wizard

**Terminal List**

Please select terminals to manage by power user
You can add or delete terminals form privilege properties page.

List of node can be

| Terminal ID | Terminal Name | Terminal Status |
|---|---|---|
| 50 | Terminal 50 | Normal |
| 70 | Terminal 70 | Normal |

| Terminal ID | Terminal Name |
|---|---|

Privilege Registration Wizard

**User List**

Please select users to manage by power user
You can add or delete users form privilege properties page.

List of users can be

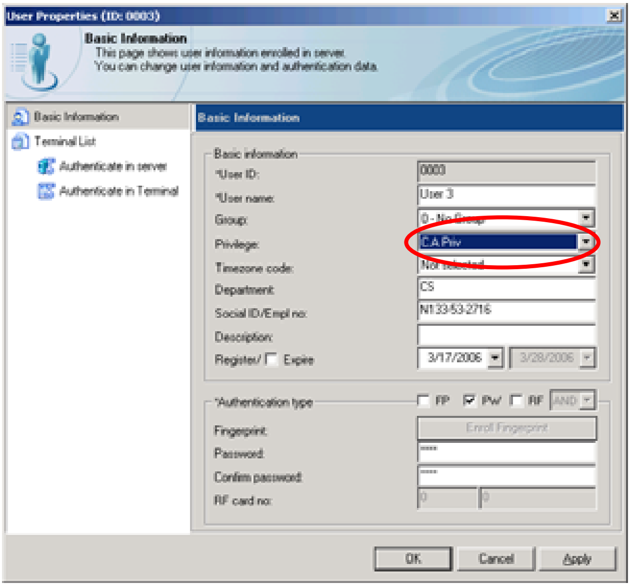
| User ID | User Name |
|---|---|
| 0002 | User 2 |
| 0003 | User 3 |

| User ID | User Name |
|---|---|
| 0001 | User 1 |

**<Create(C)>**: registration will be completed by clicking the button and new privilege can be registered again.

**<Close(O)>:** the progresses that have been made before the button is clicked will be cancelled.

The created privileges are applied to user information. The designated users with privilege can use the selected functions and can manage users as well as terminals after login.



User Properties (ID: 0003)

Basic Information

This page shows user information enrolled in server.
You can change user information and authentication data.

Basic information

*User ID: 0003

*User name: User 3

Group: 0 - No Group

Privilege: C.A Priv

Timezone code: Not selected

Department: CS

Social ID/Empl no: N133-53-2716

Description:

Register/ □ Expire: 3/17/2006 3/28/2006

*Authentication type: □ FP ☑ PW □ RF AND

Fingerprint:

Password: ****

Confirm password: ****

RF card no: 0 0

Basically, users subject to management include general users and visitors.

Semi-administrator or administrators can be included in the group, however, it is not recommended to include them in order to ensure easy management. The following steps will enable the inclusion of administrator and power user.

(1) Include general users in the list of users subject to management.

(2) Then, an administrator will change the privilege of the users into administrator or power user under user information.

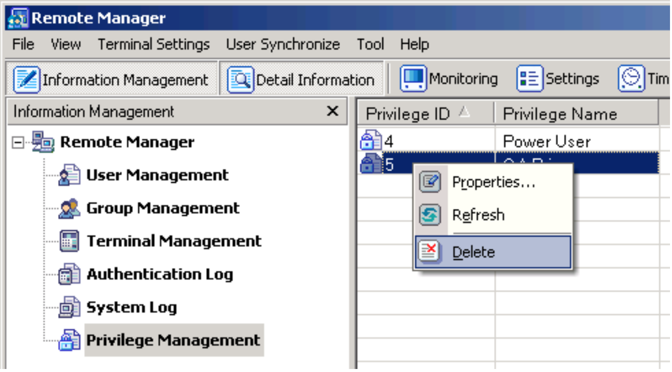
However, it is impossible to modify the privilege of these users.

## ■ To delete privilege

The following steps will delete privileges.

(1) Please select "privilege management" in an "information management" window.

(2) After selecting the groups to be deleted from the list, please select a delete button from tool bar or use a **<delete>** key from a keyboard. You can also use a right mouse click to select delete.



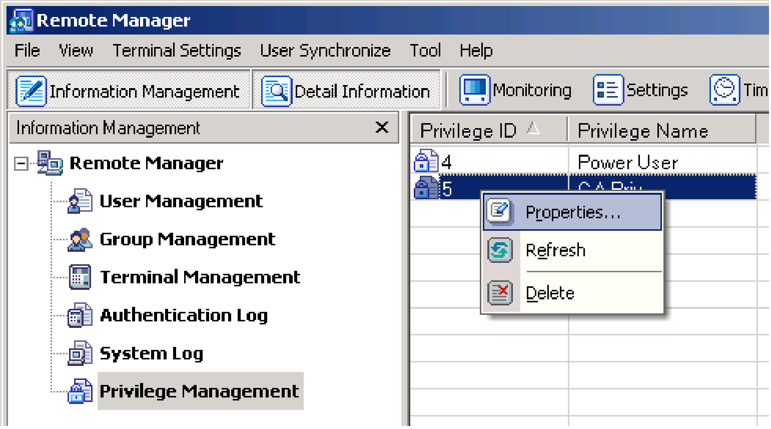
In order to delete privilege of a number of users, please use **<Shift> or <Ctrl>** key to select a multiple number of groups.

## ■ To confirm/modify information on registered privilege.

You can confirm or change settings for basic privilege, users and terminals.

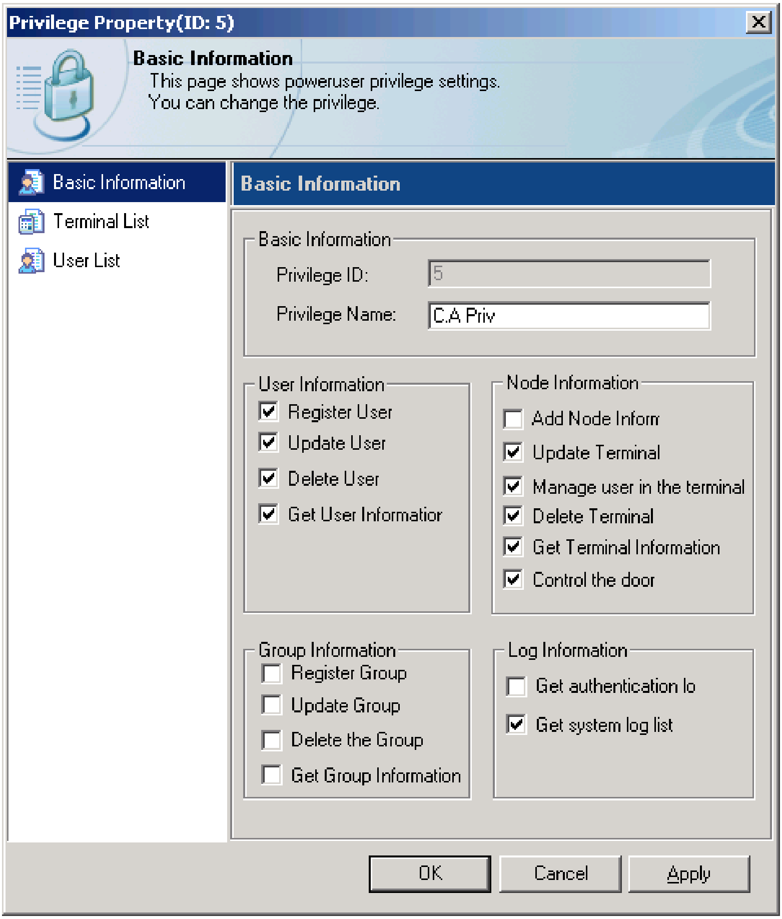
(1) Please select **<Group Management>** in an information management window.

(2) Please double click the relevant group from the list or use a right mouse click to select **<Properties…>**.



(3) When the following <Properties…> window opens, you can change basic information setting. In order to add or delete users or terminals, please select <User list> or <Terminal List> from the menu in the left.

The rest of the steps are equal to the privilege registration procedures explained earlier.



Privilege Property(ID: 5)

**Basic Information**

This page shows poweruser privilege settings.
You can change the privilege.

**Basic Information**

Basic Information

Privilege ID: 5

Privilege Name: C.A Priv

User Information

- ☑ Register User
- ☑ Update User
- ☑ Delete User
- ☑ Get User Informatior

Node Information

- □ Add Node Inform
- ☑ Update Terminal
- ☑ Manage user in the terminal
- ☑ Delete Terminal
- ☑ Get Terminal Information
- ☑ Control the door

Group Information

- □ Register Group
- □ Update Group
- □ Delete the Group
- □ Get Group Information

Log Information

- □ Get authentication lo
- ☑ Get system log list

## 4.8 Anti Pass Back

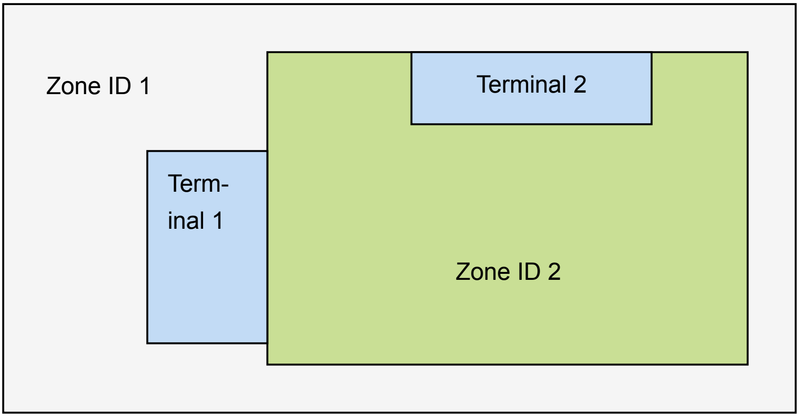
Anti Pass Back is a type of access control when users access an A/S zone. They cannot have an access in and out of a place without authentication. (access will be allowed only with authentication)

Access Manager provides Anti Pass Back by zone in order to do the above.

What is Anti Pass Back by zone?

When authentication took place at an entrance to zone A, users can move to zone B only when they get authentication at an exit of zone A. If they try to move to zone B without authentication, Anti Pass Back Error occurs.

### ■ What is an Area



The illustration will help you understand how it operates better.
As the above illustration explains, terminal 1 is an exit for an external zone (zone 1) and also an entrance to zone 2.

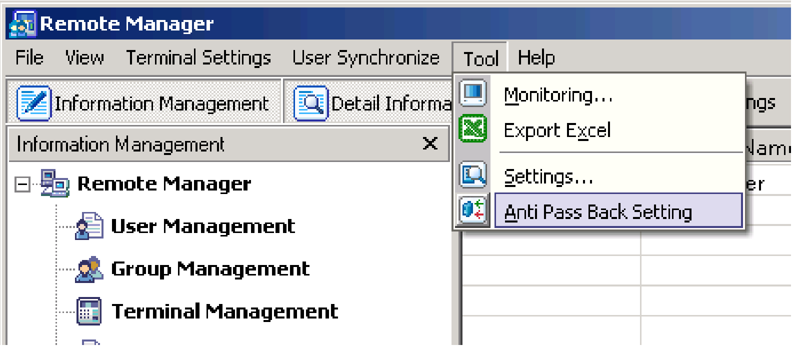
Terminal 2 is an exit of zone 2 and also an entrance to an external zone.

In order to apply Anti Pass Back, it is necessary to set an exit and entrance to a zone by terminal. When such terminals are set, there should be more than one terminal that is compled with those terminals. The above illustration is the simpliest concept and more terminals can be set for multiple zones.

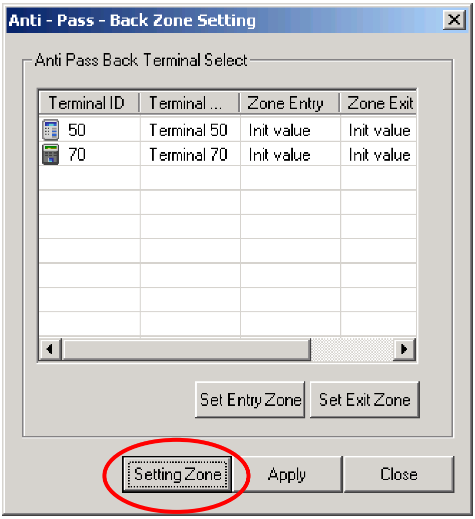
From user’s perspective, the initial value for Anti Pass Back is 0. If the user enters into zone 2 through terminal 1, the value for Anti Pass Back changes into 2(ID for the zone.) In this case, Anti Pass Back error occurs in other terminals if the user gets out of the zone without authentication from terminal 2. Yet, the value of Anti Pass Back changes into 1 if the user gets out of the zone through terminal 2.

In order to have the above illustrated setting, please follow the next steps.

## ■ Zone Setting



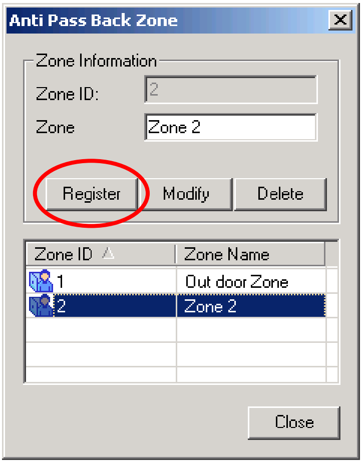
(1) Please click **<Anti Pass Back Setting>** from tools in the menu bar.


Anti - Pass - Back Zone Setting
Anti Pass Back Terminal Select
Set Entry Zone
Set Exit Zone
Setting Zone
Apply
Close

| Terminal ID | Terminal ... | Zone Entry | Zone Exit |
|---|---|---|---|
| 50 | Terminal 50 | Init value | Init value |
| 70 | Terminal 70 | Init value | Init value |

<Illustration 1>

(2) Please select **<Setting Zone>** button from <Illustration 1> in order to activate the following window for zone editing.



Anti Pass Back Zone

Zone Information

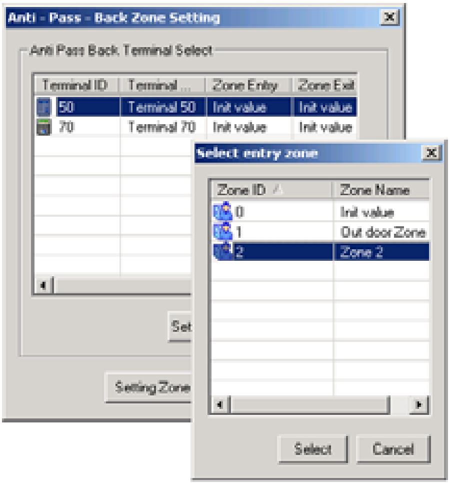
Zone ID: 2

Zone: Zone 2

| Zone ID | Zone Name |
|---|---|
| 1 | Out door Zone |
| 2 | Zone 2 |

When a zone registration window opens after clicking **<Register>**, please type in zone ID and zone name to proceed. As ID 1 is a default for external zones, you cannot modify or delete it.

(3) When zone registration is done, please select terminals for each zone. After clicking target terminals from <illustration 1>, please set entrance and exits for each zone by clicking relevant buttons.



Anti - Pass - Back Zone Setting

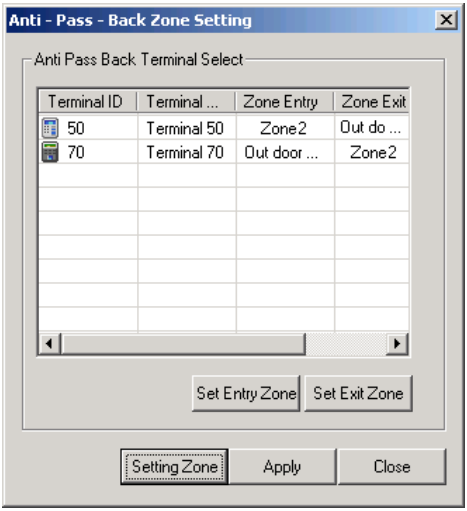
Anti Pass Back Terminal Select

| Terminal ID | Terminal ... | Zone Entry | Zone Exit |
|---|---|---|---|
| 50 | Terminal 50 | Init value | Init value |
| 70 | Terminal 70 | Init value | Init value |

Select entry zone

| Zone ID | Zone Name |
|---|---|
| 0 | Init value |
| 1 | Out door Zone |
| 2 | Zone 2 |

When you set entrance and exit to zones, you will have the following screen.



Anti - Pass - Back Zone Setting

Anti Pass Back Terminal Select

| Terminal ID | Terminal ... | Zone Entry | Zone Exit |
|---|---|---|---|
| 50 | Terminal 50 | Zone2 | Out do ... |
| 70 | Terminal 70 | Out door ... | Zone2 |

Please click an <apply> button to complete the setting.

- **Note**

1. Please make sure that you select an exit when you selected an entrance to a zone.

2. Please make sure that you select an entrance when you selected an exit to a zone.

3. Please do not select the same values for an exit and an entrance to a zone.

## ■ Network Errors

As Anti Pass Back function operates on a network, errors occur if a relevant terminal is disconnected from the network.

Therefore, the following policies are in place.

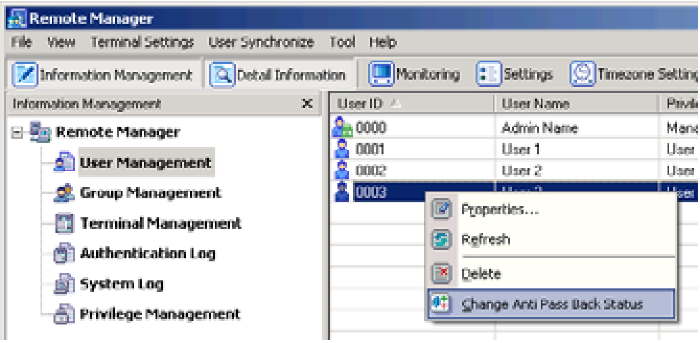
### • Anti Pass Back Level

If terminals at an exit or entrance to a zone are disconnected from a server or are not in a normal status, users cannot pass through different exits or entrances including the relevant zone because of Anti Pass Back setting.

If Anti Pass Back Level is selected at **<low>** in the above case, users can pass through entrances and exits associated with the relevant zone in case of network errors (default value). If the level is set at **<high>,** users cannot pass through entrances or exits.

### • Initialization in case of errors

Please select a user management item from information management window, and select a user. A right mnouse click to initialize Anti Pass Back will enable one access regardless of APB.



⚠ Anti Pass Back should be set when all terminals are connected.
If it is set when a network is disconnected, it may not operate normally.

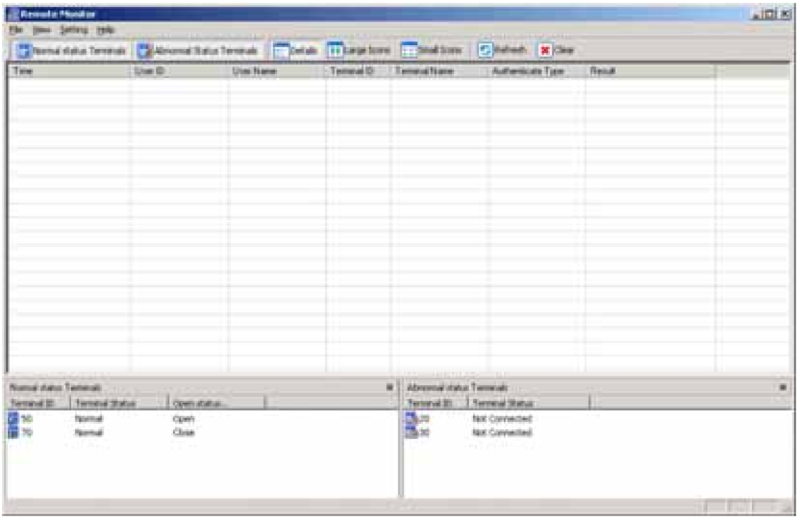
⚠ Please take note of the fact that Anti Pass Back is not applicable for NAC-3000.

## 4.9 Terminal Monitoring

You can monitor terminal status from a remote location. You can use either Remote Manager or Remote Monitor.

If you use Remote Manager, select **Monitoring** from the **Tool bar**. If you run Remote Monitor, the below window will appear.

To run Remote Monitor independently, you need to pass manager authentication.



| Time | User ID | User Name | Terminal ID | Terminal Name | Authenticate Type | Result |
|---|---|---|---|---|---|---|

Normal status Terminals

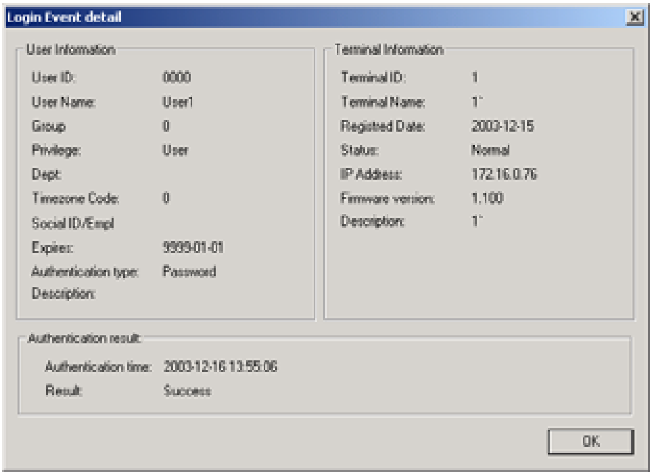
| Terminal ID | Terminal Status | Open status |
|---|---|---|
| 50 | Normal | Open |
| 70 | Normal | Close |

Abnormal status Terminals

| Terminal ID | Terminal Status |
|---|---|
| 20 | Not Connected |
| 30 | Not Connected |

As shown in the above window, you can monitor the terminal authentication log and terminal status. By clicking the buttons in the toolbar, you can configure the window as you need.

Double-click an item in the authentication log list to open the below window that provides detailed information.



Login Event detail

User Information

User ID: 0000

User Name: User1

Group: 0

Privilege: User

Dept:

Timezone Code: 0

Social ID/Empl

Expires: 9999-01-01

Authentication type: Password

Description:

Terminal Information

Terminal ID: 1

Terminal Name: 1`

Registred Date: 2003-12-15

Status: Normal

IP Address: 172.16.0.76

Firmware version: 1.100

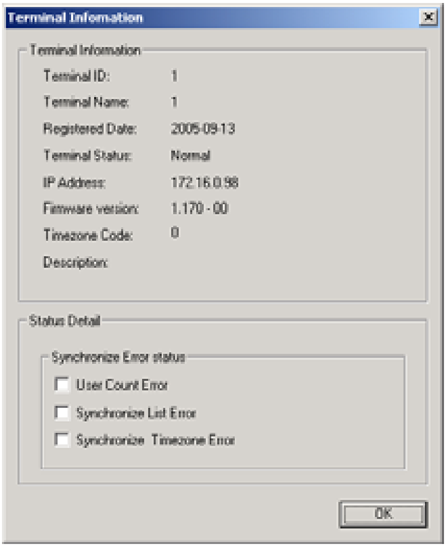
Description: 1`

Authentication result

Authentication time: 2003-12-16 13:55:06

Result: Success

Double-click an item in the terminal list to open the below window that provides detailed information.



Terminal Information

Terminal Information

Terminal ID: 1

Terminal Name: 1

Registered Date: 2005-09-13

Terminal Status: Normal

IP Address: 172.16.0.98

Firmware version: 1.170 - 00

Timezone Code: 0

Description:

Status Detail

Synchronize Error status

☐ User Count Error

☐ Synchronize List Error

☐ Synchronize  Timezone Error

In the monitoring program, you can additionally check the door status.

## ■ Description of icons

| Terminal status | Description |
|---|---|
|  | The terminal is in normal status while the door is open. |
|  | The terminal is in normal status while the door is closed. |
| # | The terminal has a synchronization error while the door is open. |
| # | The terminal has a synchronization error while the door is closed. |
| ? | The terminal is connected, but not registered. |
| ✗ | The terminal is not connected. |
| ! | The terminal has other errors. |

⚠ The door open/closed status indication feature may not be supported for some types of doors. In this case, the door may always be in an open or closed status.

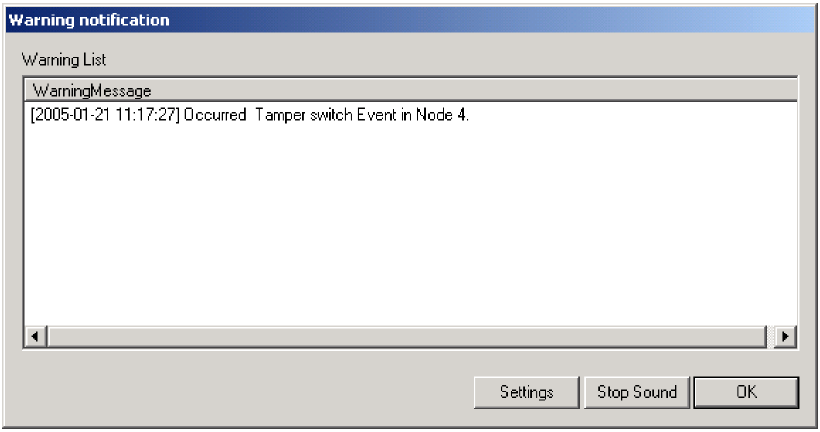
⚠ The door open/closed status icons can be viewed only in the remote monitor program.

## ■ Warning option

Remote Monitor has a feature to issue a warning.

(1) when the installed terminal is canceled
(2) when door warning is issued
(3) when door is forcefully open

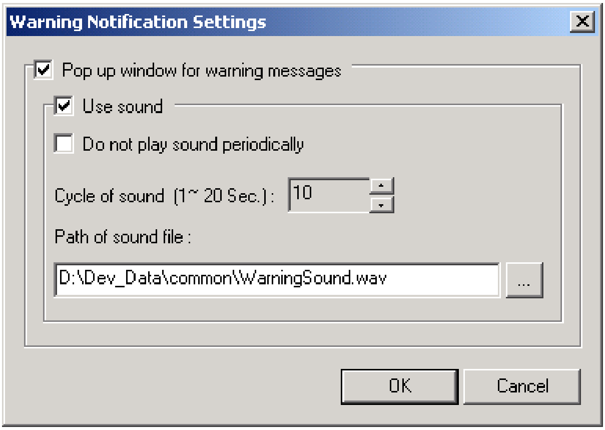
If a warning is issued, a warning message window can be displayed and a warning sound can be played depending on the warning notification settings.



[2005-01-21 11:17:27] Occurred  Tamper switch Event in Node 4.

- **Warning Notification Settings**

From Remote Monitor, select **Setting > Warning Notification Settings**.



Warning Notification Settings

☑ Pop up window for warning messages

☑ Use sound

□ Do not play sound periodically

Cycle of sound (1~ 20 Sec.) : 10

Path of sound file :

D:\Dev_Data\common\WarningSound.wav

(1) Pop up window for warning messages

If you select this option, a window will appear whenever a warning message comes in.

(2) Use sound

You can select this option when **Pop up window for warning messages** is selected.

(3) Do not play sound periodically

If a warning message comes in, the warning sound will be played only once.

(4) Cycle of sound

If **Do not play sound periodically** is not selected, the warning sound will be played periodically. Depending on the length of the warning sound, the cycle can be set at between 1 and 20 seconds.

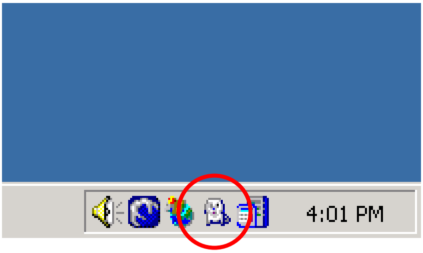
(5) Path of sound file

You can select a warning sound file other than the default one. (WarningSound.wav)

## 4.10 Watchdog

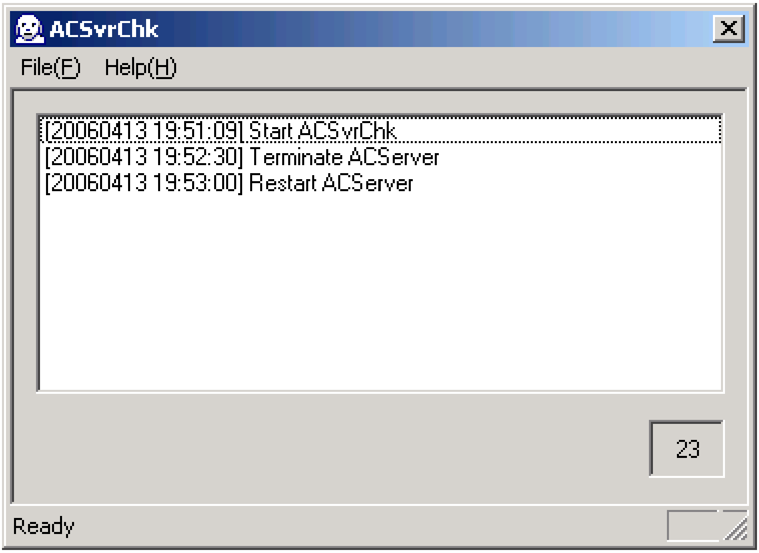
Access server watchdog program will monitor the access server to support and ensure normal operation of access server.
Server watchdog program will check the system at a regular interval. If access server is not running, the watchdog will initiate the access server.
When access server is running, the server watchdog program will be automatically running.

The following shows a window to run server watchdog program.



- How to View the History: **Show History**
  Do a right click on tray icons of the server watchdog program, and then select <History Show> menu which will show a brief history of the program.

  The following is a window to run <Show History>.



```
[20060413 19:51:09] Start ACSvrChk
[20060413 19:52:30] Terminate ACServer
[20060413 19:53:00] Restart ACServer
```

- **Close**

  Do a right click on tray icons of the server watchdog program and then select **<Close>** menu to close the program.

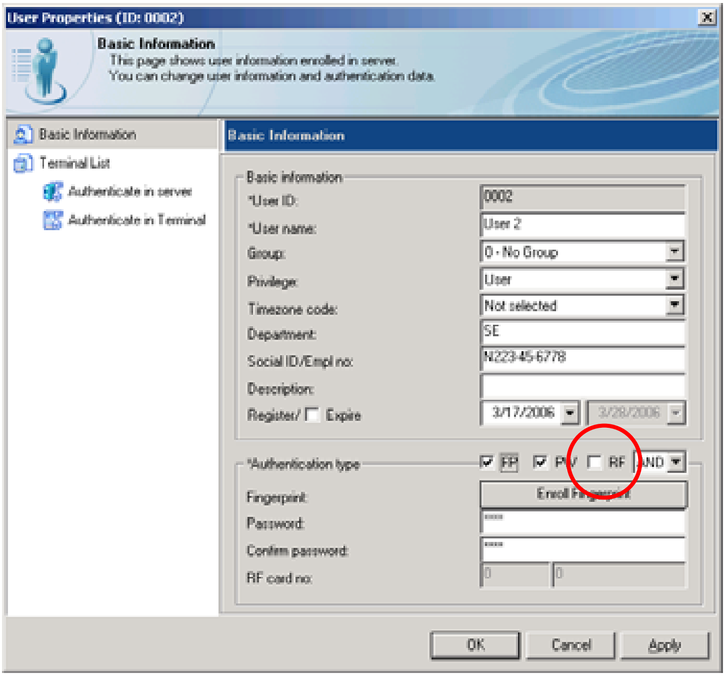
  When the Access server is closed in a normal manner, the werver watchdog program will be automatically shut down.

# APPENDIX.1 How to register RF card

In order to register RF card in Access Manager, you have to know the site code and serial number of RF card.

Serial Number is 5 digit-long back number printed on the card.
Site Code would be checked by the following step.

1. Register one RF card at your discretion on the terminal.
   (Refer to **Terminal User Manual**.)
2. Select **User Management** out of Access Manager.
3. Registered user on a terminal would be seen.
4. When you double-click user name registered with RF card or choose **Properties**, the below window would be displayed.



User Properties (ID: 0002)

Basic Information
This page shows user information enrolled in server.
You can change user information and authentication data.

Basic information
*User ID: 0002
*User name: User 2
Group: 0 - No Group
Privilege: User
Timezone code: Not selected
Department: SE
Social ID/Empl no: N223-45-6778
Description:
Register/ □ Expire 3/17/2006 3/28/2006

*Authentication type ☑ FP ☑ PW □ RF AND
Fingerprint: Enroll Fingerprint
Password: ****
Confirm password: ****
RF card no: 0 0

5. 2 digit-long front number is Site code in a card.

⚠ If 4 digit-long front codes on a card are same, site code will be identical. For example, site code of S003-12345 and S003-23456 would be same.

# APPENDIX.2 FAQ (Frequently Asked Question)

**Fingerprint authentication does not work. What can I do?**

1. On a cold day or right after you wash your hands, your fingerprints easily get dry. And if your hands are contaminated with dirt or dust, your fingerprints will also get dry. In these cases, apply a moisturizer to return them to their normal condition before trying fingerprint authentication.

2. When you have difficulties with fingerprint authentication, it is desirable to try the verification authentication method (enter your ID and get it compared to your original fingerprint on a 1:1 basis) rather than the identification authentication method (try authentication without entering your ID). NAC-3000 also supports SID that allows you to try authentication after pressing only first 2 digits of your ID, which provides better fingerprint recognition rate than the identification authentication method.

3. In case your fingerprint gets transformed by a wound, and thus becomes different from the saved one, you can use a password or an RF card as a supplementary authentication tool.

4. If you use the server authentication mode (NL mode) among network authentication modes and the server is also used as a personal or a business PC, the load on the PC will increase due to the additional works other than authentication, thereby decreasing the authentication rate.

**The Auto-on function does not work or malfunctions.**

1. The device does not work even if you place your fingerprint on

the fingerprint input window.

First of all, check if the Auto-on function is set to OFF. If so, change it to ON. If it does not work after you change the setting, please contact NITGEN Customer Support Center.

***NITGEN Customer Support Center (82-31-451-9400, customer@nitgen.com)***

2. The device continues to work even if you do not place your fingerprint on it.

When the LED of the fingerprint recognition device blinks repeatedly, when you reset the terminal power, the LED may blink for a certain amount of time, and the Auto-on function may not work. In this case, please contact NITGEN Customer Support Center.

3. The device malfunctions when you use the RF card.

In NAC-3000R, if you place the RF card on the terminal for authentication, the Auto-on sensor can be activated. It may happen mainly with our old-version products. In this case, please contact NITGEN Customer Support Center.

**The RF card authentication doesn't work.**

First of all, check if the RF card function is set to OFF. If so, change it to ON. If it does not work after you change the setting, please contact NITGEN Customer Support Center.

**How can I upgrade the firmware?**

Use Access Manager to download the firmware (binary file) provided by NITGEN from the server to the terminal.
(using TCP/IP)

**The terminal makes a buzz.**

Depending on the type of the interphone connected to NAC-3000, there may be serious howling. If you use Kocom's interphone (DP-202H) that has proven compatibility with NAC-3000, howling can be eliminated.

**Is there any countermeasure against static electricity?**

NAC-3000 obtained CE certification with regard to ESD (Electro Static Discharge), and passed the internal QA certification test. So we guarantee that this device satisfies Level 3 (Contact: 6kV, Air: 8kV) of the IEC 61000-4-2 standard. However, if it is installed in wintertime or in a place with low humidity and carpeted floor, 35kV of static electricity can be discharged to people. So please exercise caution when using the device in such an environment.

**What can I do if the device is destroyed by an intruder?**

Depending on installation methods, NAC-3000 can be categorized into the general type and the buried type. As the buried type is kept inside the wall, it is safe from accidental damage. The general type is protected with a metal bracket and cannot be damaged easily. However, in case someone tries to destroy or disassemble it by force, the tamper switch works with alarm sound.